Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Privacy Legislation in Canada

Two federal laws

Canadians are protected by two federal privacy laws, the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*.

The *Privacy Act* took effect on July 1, 1983. This Act imposes obligations on some 150 federal government departments and agencies to respect the privacy rights of Canadians by placing limits on the collection, use and disclosure of personal information. The *Privacy Act* gives Canadians the right to access and correct personal information about them held by these federal government organizations.

As of January 1, 2001, individuals are also protected by the *Personal Information Protection and Electronic Documents Act* which sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities.

The law gives individuals the right to see and ask for corrections to information an organization may have collected about them. Since the beginning of this year, the Act applies to personal information about customers or employees that is collected, used or disclosed by the federally regulated sector in the course of commercial activities.

It also applies to information sold across provincial and territorial boundaries. As of January 1, 2002, the personal health information collected, used or disclosed by these organizations is also covered.

As of January 1, 2004, the Act will cover the collection, use or disclosure of personal information in the course of any commercial activity within a province, including provincially regulated organizations. The federal government may exempt organizations or activities in provinces that have their own privacy laws if they are substantially similar to the federal law. To assist in making that determination, the Privacy Commissioner is mandated, under the Act, to report to Parliament on the extent to which provinces have passed legislation that is in fact substantially similar.

Oversight of both Acts rests with the Privacy Commissioner of Canada who is also authorized to receive and investigate complaints.

Provincial and Territorial Laws

Every province but Newfoundland has privacy legislation governing the collection, use and disclosure of personal information held by government agencies. All jurisdictions with personal data protection legislation provide Canadians with a general right to access and correct their personal information.

Oversight is through either an independent commissioner or ombudsman authorized to receive and investigate complaints.

How privacy is protected in the private sector

As mentioned above, the *Personal Information Protection and Electronic Documents Act* applies to the federally regulated sector. In 2004 it will apply to all organizations unless the federal government exempts an organization or activity in a province that has substantially similar legislation to the Act.

At present, Quebec is the only province with a personal data protection law in effect that applies to the provincially regulated private sector. This law, in addition to regulating the collection, use and disclosure of personal information held by commercial enterprises, also provides Quebecers with a general right of access to and correction of personal information.

On November 19, 2003, Quebec's private sector legislation was officially recognized as substantially similar. Organizations in Quebec will not be suject to PIPEDA and will instead continue to be suject to the Quebec private sector privacy law.

Oversight of the law is in the hands of the *Commission d'accès à l'information* which is authorized to receive and investigate complaints and has order-making powers.

Sector-Specific Legislation Dealing with Privacy

Some jurisdictions have enacted legislation to deal specifically with the collection, use and disclosure of personal health information by provincial health care organizations and other approved individuals and agencies. They are Alberta, Saskatchewan and Manitoba.

There are other laws that contain provisions that provide privacy protection to Canadians. The federal Bank Act, for example, contains provisions regulating the use and disclosure of personal financial information by federally regulated financial institutions. Similar restrictions can be found in provincial statutes that regulate the activities of financial institutions, such as credit unions and insurance companies in provincial jurisdiction.

Various consumer protection laws at federal and provincial levels offer limited protections and remedies against illegal and unethical business practices that may constitute an infringement of privacy.

Some provinces have privacy tort laws which provide a civil remedy for someone whose privacy has been violated.

For more information contact:

The Office of the Privacy Commissioner of Canada
112 Kent Street, Ottawa, ON K1A 1H3
Tel.: 1 (613) 995-1376
Fax 1(613) 947-6850

E-mail: info@privcom.gc.ca.
www.privcom.gc.ca
1-800-282-1376

Provincial / Territorial Privacy Laws, Oversight Offices and Government Organizations -

Revised in January 2002

Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Gearing up for the *Personal Information Protection and Electronic Documents Act*

In Canada, we are protected by two federal privacy laws. The *Privacy Act* covers the personal information-handling practices of the federal government and the *Personal Information Protection and Electronic Documents (PIPED) Act* is Canada's new private sector privacy law, which is coming fully into effect on January 1, 2004. The Office of the Privacy Commissioner of Canada is here to help provide information and guidance to businesses across Canada as they gear up for the implementation of the *PIPED Act*.

Good privacy is good business

In an increasingly competitive marketplace, businesses rely on personal information to identify and stay in touch with their customers. They use it to seek out new customers who might be interested in their products. They want to find out what the market is looking for and what it will bear. And they want information about their employees, so that they can administer benefits and ensure a safe and productive workplace.

Obtaining and using that personal information in ways that don't offend the fundamental human right of privacy is the challenge for modern businesses.

Respecting and protecting privacy is a key element of good customer relations — and that makes it a key element of competitive advantage. Your customers want privacy, your employees need it and your competitors are going to provide it.

It's not an abstract legal concept. It's simple consideration, respect and courtesy — the essence of a good relationship with your customers and employees. Showing respect for privacy is part of showing respect for your customer, and respecting your customer is the cornerstone of a strong customer relationship.

The *PIPED Act* in brief

The *PIPED Act* sets out ground rules for how private sector organizations can collect, use or disclose personal information in the course of commercial activities. It balances an individual's right to privacy with the need of organizations to collect, use or disclose personal information for legitimate business purposes.

The *PIPED Act* has been coming into effect in stages. As of January 2001, the Act has applied to personal information about customers or employees in the federally-regulated sector in the course of commercial activities. It also applies to information sold across provincial and territorial boundaries. As of January 2002, the Act has also applied to personal health information collected, used or disclosed by these organizations.

On January 1, 2004, the *PIPED Act* will apply right across the board — to all personal information collected, used or disclosed in the course of commercial activities by all private sector organizations, except provinces which have, by then, enacted legislation that is deemed to be substantially similar to the federal law. To date, Quebec is the only province with legislation that is substantially similar to the *PIPED Act*.

The basic outline of the *PIPED Act* looks like this:

- If your business wants to collect, use or disclose personal information about people, you need their consent, except in a few specific and limited circumstances.
- You can use or disclose people's personal information only for the purpose for which they gave consent.
- Even with consent, you have to limit collection, use and disclosure to purposes that a reasonable person would consider appropriate under the circumstances.
- Individuals have a right to see the personal information that your business holds about them, and to correct any inaccuracies.
- There's oversight, through the Privacy Commissioner of Canada, to ensure that the law is respected, and redress if people's rights are violated.

Your responsibilities under the *PIPED Act*

The *PIPED Act* reflects the realities of the business world. It's based on the Canadian Standards Association's *Model Code for the Protection of Personal Information*, which is incorporated into the legislation. The Code came out of a collaborative effort by representatives of government, consumers and business groups, and lists 10 principles of fair information practices, which are summarized as follows:

1. **Accountability**: Appoint an individual (or individuals) to be responsible for your organization's compliance; protect all personal information held by your organization or transferred to third party for processing; and develop and implement personal information policies and practices.
2. **Identifying purposes**: Your organization must identify the reasons for collecting personal information before or at the time of collection. Before or when any personal information is collected, identify why it is needed and how it will be used; document why the information is collected; inform the individual from whom the information is collected why it is needed; identify any new purpose for the information and obtain the individual's consent before using it.
3. **Consent**: Inform the individual in a meaningful way of the purposes for the collection, use or disclosure of personal data; obtain the individual's consent before or at the time of collection, as well as when a new use is identified.
4. **Limiting collection**: Do not collect personal information indiscriminately; do not deceive or mislead individuals about the reasons for collecting personal information.
5. **Limiting use, disclosure, and retention**: Use or disclose personal information only for the purpose for which it was collected, unless the individual consents, or the use or disclosure is authorized by the Act; keep personal information only as long as necessary to satisfy the purposes; put guidelines and procedures in place for retaining and destroying personal information; keep personal information used to make a decision about a person for a reasonable time period. This should allow the person to obtain the information after the decision and pursue redress; destroy, erase or render anonymous information that is no longer required for an identified purpose or a legal requirement.
6. **Accuracy**: Minimize the possibility of using incorrect information when making a decision about the individual or when disclosing information to third parties.
7. **Safeguards**: Protect personal information against loss or theft; safeguard the information from unauthorized access, disclosure, copying, use or modification; protect personal information regardless of the format in which it is held.
8. **Openness**: Inform your customers, clients and employees that you have policies and practices for the management of personal information; makethese policies and practices understandable and easily available.

105-01557/

9. **Individual access**: When requested, inform individuals if you have any personal information about them; explain how it is or has been used and provide a list of any organizations to which it has been disclosed; give individuals access to their information; correct or amend any personal information if its accuracy and completeness is challenged and found to be deficient; provide a copy of the information requested, or reasons for not providing access, subject to exception set out in Section 9 of the Act; an organization should note any disagreement on the file and advise third parties where appropriate.
10. **Provide recourse**: Develop simple and easily accessible complaint procedures; inform complainants of avenues or recourse. These include your organization's own complaint procedures, those of industry associations, regulatory bodies and the Privacy Commissioner of Canada; investigate all complaints received; take appropriate measures to correct information handling practices and policies.

Individuals who feel their privacy rights have been infringed upon can complain to the Privacy Commissioner of Canada. The Commissioner's role is that of an ombudsman, trying to find solutions to privacy problems, resolving complaints through negotiation and persuasion, and using mediation and conciliation if appropriate.

What is personal information?

Personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:

- age, name, ID numbers, income, ethnic origin, or blood type;
- opinions, evaluations, comments, social status, or disciplinary actions; and
- employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs).

Personal information does not include the name, title, business address or telephone number of an employee of an organization.

What is not covered by the Act?

- The collection, use or disclosure of personal information by federal government organizations listed under the *Privacy Act*
- Provincial or territorial governments and agents of the crown in right of a province
- An employee's name, title, business address or telephone number
- An individual's collection, use or disclosure of personal information strictly for personal purposes (e.g. personal greeting card list)
- An organization's collection, use or disclosure of personal information solely for journalistic, artistic or literary purposes

For more information

We recognize that gearing up to protect privacy isn't easy. It takes time, attention and resources. But part of our job is to help you with it.

For more information to help your business prepare for the implementation of the *PIPED Act*, contact the Office of the Privacy Commissioner of Canada at 1-800-282-1376 and request a copy of our *Guide for Businesses and Organizations: Your Privacy Responsibilities* free of charge This *Guide* also includes a *Privacy Questionnaire* with some common sense questions

you can use to help you get started.

For this and other useful information, such as the Commissioner's findings under the *PIPED Act*, you can also visit our Web site at www.privcom.gc.ca or you can write to us at:

Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, ON K1A 1H3

Last Updated: 12/19/2003 9:37:

Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

A Guide for Canadians

What is the Personal Information Protection and Electronic Documents Act?

Part 1 of the *Personal Information Protection and Electronic Documents Act* sets down the ground rules for how organizations may collect, use or disclose information about you in the course of commercial activities. The law gives you the right to see and ask for corrections to information an organization may have collected about you. If you think an organization covered by the Act is not living up to its responsibilities under the law, you have the right to lodge an official complaint.

What is personal information?

"Personal information" under the Act means information about an "identifiable individual".

For example, "personal information" includes your

- name, age, weight, height
- medical records
- income, purchases and spending habits
- race, ethnic origin and colour
- blood type, DNA code, fingerprints
- marital status and religion
- education
- home address and phone number

"Personal information" does **not** include the name, job title, business address or office telephone number of an employee of an organization that is covered by the new law.

How does the Act protect my personal information?

Your ability to control your personal information is key to your right to privacy.

The Act gives you control over your personal information by requiring organizations to obtain your consent to collect, use or disclose information about you. The Act confers certain rights on individuals, and imposes specific obligations on organizations.

The law gives you the right to:

- know why an organization collects, uses or discloses your personal information;*
- expect an organization to collect, use or disclose your personal information reasonably and appropriately, and not use the information for any purpose other than that to which you have consented;*

- know who in the organization is responsible for protecting your personal information;
- expect an organization to protect your personal information by taking appropriate security measures;
- expect the personal information an organization holds about you to be accurate, complete and up-to-date;
- obtain access to your personal information and ask for corrections;*
- complain about how an organization handles your personal information.

The law requires organizations to:

- obtain your consent when they collect, use or disclose your personal information;*
- supply you with a product or a service even if you refuse consent for the collection, use or disclosure of your personal information unless the information is essential to the transaction;*
- collect information by fair and lawful means;
- have personal information policies that are clear, understandable and readily available.

An organization should destroy, erase or make anonymous personal information about you that it no longer needs in order to fulfil the purpose for which it was collected.

*There are exceptions to these principles. For example: an organization may not need to obtain your consent if collecting the information clearly benefits you and your consent cannot be obtained in a timely way; or if the information is needed by a law enforcement agency for an investigation, and getting consent might compromise the information's accuracy.

How can I see the personal information an organization has about me?

- Send a written request to the organization holding your personal information. You must provide enough detail to allow the organization to identify the information you want; for example, include dates, account numbers, and the names or positions of people you may have dealt with at the organization.
- Organizations must provide the information requested within a reasonable time and at minimal or no cost.

How can I correct errors or omissions in my personal information?

- Write to the organization that has personal information about you and explain the correction you are requesting and why. Supply copies of any documents that support your request, if you have them.
- If the organization refuses to correct your personal information, you may require it to attach a statement of your disagreement to the file. This statement must be passed on to any other organization that may have access to the information.

What if I believe my privacy rights are being abused?

The Act gives you the right to make a complaint if:

- you run into any difficulties obtaining your personal information, if an organization refuses to correct information you consider inaccurate or incomplete, or if you suspect your personal information has been improperly collected, used or disclosed;
- you believe an organization is not following any provision of the law.

Where do I complain?

- Contact the Office of the Privacy Commissioner of Canada during business hours by calling 1 800 282-1376 if you need more information and advice on how you should proceed.
- We encourage you to try to settle the matter directly with the organization about which you are complaining by contacting the person responsible for handling privacy issues within the organization.
- If you are not satisfied with the organization's response, you may contact the organization's industry association, ombudsman or complaint office, if there is one. For example, the Canadian Marketing Association and the Canadian Banking Ombudsman handle customers' complaints about their member companies.
- If you are not satisfied with the way the organization or industry association handles the matter, contact the Privacy Commissioner of Canada. There is no fee for making a complaint to Privacy Commissioner.

What is the role of the Privacy Commissioner of Canada?

- The Privacy Commissioner is an ombudsman who attempts to resolve disputes through negotiation.
- The Commissioner has the power to investigate your complaint.
- The Commissioner may also initiate his own investigation or review how an organization handles personal information.
- The Commissioner can recommend that the organization release your personal information to you or correct inaccuracies.
- The Commissioner can recommend that organizations change their personal information practices.
- The Commissioner will report the findings of the investigation to you and the organization.

What if the organization ignores the recommendations of the Privacy Commissioner?

- The Privacy Commissioner has the power to make public any information about the personal information practices of an organization. Few businesses would like to be publicly identified as violating the privacy rights of individuals.
- The Privacy Commissioner may also take the complaint to the Federal Court of Canada on your behalf if he supports you but has been unable to resolve the dispute.
- Once you have received the Privacy Commissioner's report, you may, under certain circumstances, take your complaint to the Federal Court of Canada yourself.
- The Court can order an organization to correct any practices that do not comply with the law, and to publish notices of how it has or will correct its practices.
- The Court can also award damages to the complainant including damages for humiliation suffered.

What is NOT COVERED by the Personal Information Protection and Electronic Documents Act?

- Any federal government organization already covered by the *Privacy Act*.
- Provincial or territorial governments, and their agents.

- Any organization that collects, uses or discloses personal information solely for journalistic, artistic or literary purposes.
- An individual's collection, use or disclosure of personal information for personal purposes, such as genealogical research shared with other family members.

When does the Act come into force?

The Act takes effect in three stages spread over three years.

January 1, 2001
At this stage, the Act applies to personal information about customers or employees (except "personal health information") that is collected, used or disclosed by "federal works, undertakings or businesses" in the course of commercial activities.

(Federal works, undertakings and businesses include organizations such as the banks, telephone companies, cable television and broadcasting companies, firms engaged in interprovincial transportation, and air carriers.)

The Act also applies to personal information that is shared or disclosed for profit or any kind of benefit across the borders of Canada or a province, where the information itself is the subject of the transaction.

The Act also covers all businesses and organizations engaged in commercial activity in Yukon, the Northwest Territories and Nunavut.

January 1, 2002
The Act will cover any "personal health information" collected by those organizations mentioned in the first stage. Personal health information is information about an individual's mental or physical health, including details about any tests, examinations and health services provided.

January 1, 2004
The Act will cover the collection, use or disclosure of personal information in the course of any commercial activity within a province, including provincially regulated enterprises such as retail stores. The federal government may exempt organizations and/or activities in provinces that have their own privacy laws that are substantially similar to the federal law.

The Act will apply to all personal information in all interprovincial and international transactions by all organizations in the course of their commercial activities.

FOR MORE INFORMATION

If you have any questions about how a private sector organization handles your personal information or wish to make a complaint under the new law, please contact our office.

The Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario K1A 1H3

Telephone: 1 (613) 995-8210
Toll-free: 1 800 282-1376
Fax: 1 (613) 947-6850
Web site: www.privcom.gc.ca
E-mail: info@privcom.gc.ca

Please note that this brochure summarizes the law. As such, it has no legal status. To obtain the full text of the law, consult our Web site or contact the Office of the Privacy Commissioner of Canada.

Cette publication est disponible également en français.

February 2001

Last Updated: 12/19/2003 10:27

Fact Sheets

Protecting Your Personal Information

In this age of electronic information storage and powerful computers, your personal information can be collected, shared and matched with a click of a button.

Canada has two federal privacy laws in place to protect your personal information.

With these, you can find out why your personal information is being collected, how it's being used, where your information is stored and to whom it is disclosed.

You also can access your personal information and even lodge a complaint if you are unhappy with how an organization is handling your information.

However, maintaining as much control as possible over your personal information can go a long way toward protecting your privacy.

How to protect your personal information

We often give out our name, address and phone number without a second thought. In a perfect world, companies would protect your personal information. Unfortunately, this is not often the case.

Below are some practical tips on how you can protect your personal information yourself:

- Always read the fine print on sales agreements. By signing you may also be giving the organization permission to add your name to a marketing list. Check the "no thanks" box, or write and initial a short note on the document saying you don't want your personal information shared with anyone else.
- Many retail stores ask for your name, address and telephone number when you make a purchase. If the store cannot give you a satisfactory reason for collecting the information, don't give it out.
- Information collected on product warranty cards is very often used for marketing purposes. You are not required to send in a filled warranty card - your receipt is all you need to make a warranty claim.
- Charities and other fund-raising organizations often share donor lists with one another. If you make a donation and do not want your personal information to be given to any other charities, enclose a note with your payment.
- If you don't want your personal information out there, avoid filling out ballots for "free draws" or other promotions. These are surefire ways to get your name, address and telephone number on a junk mail or telemarketing list.
- Many stores offer "rewards" or "points" programs. Often stores see your participation as consent to share your information without directly asking for your permission. If you want to avoid getting junk mail or other promotional material, either don't join these programs, or ask the stores not to share your personal information.
- Look through a copy of any magazines to which you subscribe. Most mention they may give your name and address to other companies for one reason or another. They also offer you the opportunity to opt out of this "service". Do it!
- Every time you make a call, dial *67 on your telephone (1167 on old rotary dial phones) to prevent your name and number from being displayed.
- You may be able to remove your name from many mailing and telephone lists by writing to the Canadian Marketing Association, 1 Concorde Gate, Suite 607, Don Mills, Ontario, M3C 3N6.

For more information, contact:

The Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, ON
K1A 1H3
info@privcom.gc.ca
www.privcom.gc.ca
1-800-282-1376

July 2001

Last Updated: 2004-03-31 ▲ Important Notices

Fact Sheets

Best Practices for dealing with pre-PIPEDA personal information (grandfathering)

How does the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) apply to personal information collected before the Act came into effect?

The answer, in brief, is that all provisions of *PIPEDA*, including the consent principle, apply to all personal information held by an organization, regardless of when the information was collected. This means, among other things, that organizations are required to keep the information as accurate, complete and up-to-date as necessary, protect the information with appropriate safeguards and give individuals access to their personal information.

However, it does not necessarily follow that an organization must seek established customers' *express* consent to the continued retention, use or disclosure of their personal information.

Although the guidelines that follow are primarily intended to deal with customer information collected prior to the implementation of *PIPEDA*, they are equally appropriate for information relating to clients, employees, donors and other individuals, keeping in mind that *PIPEDA* only applies to employee information collected, used or disclosed by federal works, undertakings or businesses.

Purging obsolete files

In some cases, destroying or erasing older files may be the most appropriate and straightforward way to deal with them.

Under Principle 4.5 of the Act, an organization should retain personal information only as long as necessary for the fulfillment of the purposes for which it was collected; should develop guidelines and procedures regarding retention, including minimum and maximum retention periods; and should destroy or erase any personal information no longer required to fulfil identified purposes.

In determining how to treat an existing customer file, an organization should first consider such questions as:

- Is the information still serving (or has it ever served) any purpose that could reasonably be considered necessary or useful;
- Is there a legal or contractual requirement to retain the information: and
- Would the individual reasonably expect the organization to be still holding the information on file?

If the answer to any of these questions is no then the most appropriate action may be simply to purge the file. The organization should also set reasonable minimum and maximum retention periods for handling all customer files in

future.

Seeking Consent

The extent to which an organization is obliged to seek express consent from established customers depends on several considerations:

- Whether the organization made a reasonable effort to inform the customer of its purposes at the time of collecting the personal information;
- Whether the information is still being used or disclosed, and if so whether it is being used or disclosed for the same purposes for which it was collected;
- Whether the information is being used or disclosed for unidentified secondary purposes; and
- Whether the customer would reasonably expect the organization to continue using or disclosing the information for its current purposes.

These considerations relate to the purposes for which the information is being used or disclosed, the degree to which these purposes were specified at the time of collection and the reasonable expectations of the individual.

Purposes duly specified

If the organization made a reasonable effort to specify its purposes to customers at the time of collecting personal information, and if the information is still being used or disclosed for those original purposes and no others, then the organization may take the customers' consent to the purposes as implied. Provided that the information is not used or disclosed for new purposes, there is no further requirement to obtain consent.

Purposes unspecified but reasonably expected

Even if purposes were not clearly specified at the time, but if they were such as customers would reasonably have expected to be involved in the provision of the products or services concerned, then the organization may take customers' consent to the purposes as implied. (The use of personal information to fulfill a magazine subscription is an obvious example.) No further consent is required unless the organization intends to use or disclose the information for new purposes.

Purposes unspecified and not reasonably expected

If the personal information was collected for unspecified purposes that customers would not have reasonably expected to be involved in the provision of the products or services concerned (e.g., secondary purposes such as marketing or disclosures to third parties), then the organization must obtain the customers' express consent to any continued use or disclosure of the information.

New purposes

Regardless of whether the personal information was collected before or after *PIPEDA* took effect, an organization must seek customers' consent to any new use or disclosure of their personal information. A new use or disclosure is defined as any use or disclosure for purposes other than those for which personal information was originally collected.

Access to personal information

Under Principle 4.9 of *PIPEDA* , an organization must, upon request, inform individuals of the existence, use, and disclosure of their personal information, give them access to such information, and enable them to challenge its accuracy and completeness and, if required, have it amended.

This principle applies to all personal information held by an organization, regardless of when it was collected. Customers have a clear right of access to personal information collected by an organization before it became subject to *PIPEDA* .

Making privacy policies available

Under Principles 4.1 and 4.8 of *PIPEDA* , an organization must formulate privacy policies and practices and make information about them readily available to individuals.

These principles apply as much to an organization's established customers as to its new customers. It is recommended that organizations provide privacy information to new customers on the first occasion of collecting personal information from them, and to established customers at the earliest opportunity in the usual course of business communications.

Last Updated: 2004-08-19 ▲ Important Notices

Resource Centre

Privacy Questionnaire: Is Your Business Ready?

This Questionnaire is an excerpt from Your Privacy Responsibilities: A Guide for Businesses and Organizations to the *Personal Information Protection and Electronic Documents Act*.

The following are some common sense questions you can use to help your organization prepare for implementation of the *Personal Information Protection and Electronic Documents Act*.

Not all of the following questions will apply to all organizations, as the Act applies to a wide variety and size of organizations. Consider each question along with your organization's current practices. Answering "no" indicates areas that need to be addressed or improved.

Personal information holdings

- Do you know what personal information is?
- Do you collect, use or disclose personal information in your day-to-day commercial activities?
- Do you have an inventory of your personal information holdings?
- Do you know where personal information is held (physical locations and files)?
- Do you know in what format(s) the personal information is kept electronic, paper, etc.)?
- Do you know who has access to personal information in and outside your organization?

Accountability of organization and staff

- Have you named a privacy officer who is responsible for your organization's overall compliance with the Act?
- Is this responsibility shared with more than one person?
- If these responsibilities are shared, have they been clearly identified?
- Can your staff respond to internal and external privacy questions on behalf of the organization, or do they know who should respond?
- Does your staff know who receives and responds to:
  - requests for personal information?
  - requests for correction?
  - complaints from the public?
- Do your customers know whom to contact:
  - for general inquiries regarding their personal information?
  - to request their personal information?
  - to request corrections to their personal information?
  - for complaints?
- Is your privacy officer able to explain to the public the steps and procedures for requesting personal information and filing complaints?
- Has your staff been trained on the Act?
- Will there be ongoing training?
- Is your staff able to explain the purposes for the collection, use and disclosure of personal information to customers in easy to understand terms?

- Is your staff able to explain to customers when and how they may withdraw consent and what the consequences, if any, there are of such a withdrawal?
- Will you inform your employees of new privacy issues raised by technological changes, internal reviews, public complaints and decisions of the courts?

Information for customers and employees

- Do you have documents that explain your personal information practices and procedures to your customers?
- Does this information include how to:
  - obtain personal information?
  - correct personal information?
  - make an inquiry or complaint?
- Does this information describe personal information that is:
  - held by the organization and how it is used?
  - disclosed to subsidiaries and other third parties?
- Do you have a privacy policy for your web site?
- Is your privacy policy prominent and easy to find? Is it easily understandable?
- Do your application forms, questionnaires, survey forms, pamphlets and brochures clearly state the purposes for the collection, use or disclosure of personal information?
- Have you reviewed all your public information material to ensure that any sections concerning personal information are clear and understandable?
- Have you ensured that the public can obtain this information easily and without cost?
- Is this information reviewed regularly to ensure that it is accurate, complete and up to date?
- Does this information include the current name or title of the person who is responsible for overseeing compliance with the Act?

Limiting collection, use, disclosure and retention to identified purposes

- Have you identified the purposes for collecting personal information?
- Are these purposes identified at or before the time the information is collected?
- Do you collect only the personal information needed for identified purposes?
- Do you document the purposes for which personal information is collected?
- If you gather and combine personal information from more than one source, do you ensure that the original purposes have not changed?
- Have you developed a timetable for retaining and disposing of personal information?
- When you no longer require personal information for the identified purposes or it is no longer required by law, do you destroy, erase or make it anonymous?

Consent

- Does your staff know that an individual's consent must be obtained before or at the time they collect personal information?
- Does your staff know they must obtain an individual's consent before any new use or new disclosure of the information?
- Do you use express consent whenever possible, and in all cases where the information is sensitive or the individual would reasonably expect it?
- Is your consent statement worded clearly, so that an individual can understand the purpose of the collection, use or disclosure?
- Do you make it clear to customers that they need not provide personal information that is not essential to the purpose of the collection, use or disclosure?

Third party transfers

- Do you use contracts to ensure the protection of personal information transferred to a third party for processing?
- Does the contract limit the third party's use of information to purposes necessary to

fulfil the contract?

- Does the contract require the third party to refer any requests for access or complaints about the information transferred to you?
- Does the contract specify how and when a third party is to dispose of or return any personal information it receives?

Ensuring accuracy

- Is personal information sufficiently accurate, complete and up to date to minimize the possibility that your organization might use inappropriate information?
- Does your organization document when and how personal information is updated, to ensure its accuracy?
- Do you ensure that personal information received from a third party is accurate and complete?

Safeguards

- Have you reviewed your physical, technological and organizational security measures?
- Do they prevent improper access, modification, collection, use, disclosure and/or disposal of personal information?
- Is personal information protected by security safeguards that are appropriate to the:
  - sensitivity of the information?
  - scale of distribution?
  - format of the information?
  - method of storage?
- Have you developed a "need-to-know" test to limit access to personal information to what is necessary to perform assigned functions?
- Has your staff been trained about security practices to protect personal information? For example, is staff aware that personal information should not be left displayed on their computer screens or desktops in their absence?
- Is your staff aware that they should properly identify individuals and establish their right to access the personal information before disclosing it?
- Do you have rules about who is permitted to add, change or delete personal information?
- Is there a records management system that assigns user accounts, access rights and security authorizations?
- Do you ensure that no unauthorized parties may dispose of, obtain access to, modify or destroy personal information?

Requests for access to personal information

- Is your staff aware of the time limits the law allows to respond to access requests?
- Can you retrieve personal information to respond to individual access requests with a minimal disruption to operations?
- Do your information systems facilitate the retrieval and accurate reporting of an individual's personal information, including disclosures to third party organizations?
- Do you provide personal information to the individual at minimal or no cost?
- Do you advise requesters of costs, if any, before personal information is retrieved?
- Do you record an individual's response to being notified of the cost of retrieving personal information?
- Do you provide personal information in a form that is generally understandable? (For example, do you explain abbreviations?)
- Does your organization have procedures for responding to requests for personal information in an alternate format (such as Braille or audio tapes)?

Handling complaints

- Can an individual easily find out how to file a complaint with you?
- Do you deal with complaints in a timely fashion?
- Do you investigate all complaints received?

- Are your customer assistance and other front-line staff able to distinguish a complaint under the law from a general inquiry? If unsure, do they discuss this with the individual?
- Do you advise individuals about all available avenues of complaints, including the Privacy Commissioner of Canada?
- Are staff responses to public inquiries, requests and complaints reviewed to ensure they are handled fairly, accurately and quickly?
- When a complaint is found to be justified, do you take appropriate corrective measures, such as amending your policies and advising staff of the outcome?

Last Updated: 2004-03-31 ▲ Important Notices

Privacy Commissioner of Canada

About Us
Commissioner's Findings
Media Centre
News Releases
Key Issues
Miscellaneous
Resource Centre
Individuals
Business
New! e-kit
Publications
Annual Reports
Provincial/Territorial Links
Health Links
Privacy Links
Speeches
Privacy Legislation
Privacy Impact Assessments
Fact Sheets
FAQs
Privacy Quiz
To Reach Us

The Application of the *Personal Information Protection and Electronic Documents Act* to Charitable and Non-Profit Organizations

Our Office is often asked about the application of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) to charities, non-profit organizations, associations and other similar organizations. In particular, many organizations and individuals want to know how the *Act* applies to fundraising and other activities such as mailing information to previous donors or members.

As of January 1, 2004, *PIPEDA* applies to every organization that collects, uses or discloses personal information in the course of commercial activities. However, the federal government may exempt organizations and/or activities in provinces that are deemed to have adopted substantially similar privacy legislation. The *Act* also applies to personal information in interprovincial and international transactions by all organizations subject to the *Act* in the course of their commercial activities.

The presence of commercial activity is the most important consideration in determining whether or not an organization is subject to the *Act*. Section 2 of the *Act* defines "commercial activity" as:

> "...any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists."

Whether or not an organization operates on a non-profit basis is not conclusive in determining the application of the Act. The term non-profit or not-for-profit is a technical term that is not found in *PIPEDA*. The bottom line is that non-profit status does not automatically exempt an organization from the application of the Act.

Most non-profits are not subject to the *Act* because they do not engage in commercial activities. This is typically the case with most charities, minor hockey associations, clubs, community groups and advocacy organizations. Collecting membership fees, organizing club activities, compiling a list of members' names and addresses, and mailing out newsletters are not considered commercial activities. Similarly, fundraising is not a commercial activity. However, some clubs, for example many golf clubs and athletic clubs, may be engaged in commercial activities which are subject to the Act.

As the definition of commercial activity makes clear, selling, bartering or leasing a membership list or a list of donors would be considered a commercial activity. As a result, consent is required for the disclosure of this information. Assuming the information would not be considered sensitive, an organization could use a clear, simple and easy-to-execute opt-out process as a means of obtaining consent.

Although the *Act* does not generally apply to charities, associations and other similar organizations, we recommend that such organizations provide their members, donors or supporters with an opportunity to decline to receive further communications.

Charities and other similar organizations should also be aware that some provinces have passed legislation similar to *PIPEDA*. Some of these laws apply to charities and other non-profit organizations.

Fact Sheets

Municipalities, Universities, Schools, and Hospitals

Our office is frequently asked about the application of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) to the activities of municipalities, universities, schools, and hospitals, often referred to as the "MUSH" sector.

The Application of the *Act*

PIPEDA applies to every organization that collects, uses or discloses personal information in the course of commercial activities. *PIPEDA* defines commercial activity as

> "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists."

The term organization "includes an association, a partnership, a person and a trade union." The definition of organization is intended to be broad and inclusive.

The federal government may exempt organizations and/or activities in provinces that are deemed to have adopted substantially similar privacy legislation. In those provinces that have passed substantially similar legislation, *PIPEDA* will continue to apply to the federally regulated private sector — such as banks, airlines, telephone and broadcasting companies, and railways — and to personal information in interprovincial and international transactions by all organizations engaged in commercial activities. To date, three provinces — Quebec, Alberta and British Columbia — have passed substantially similar legislation.

The MUSH Sector

The *Constitution Act, 1867* gives the provinces authority over municipal institutions, education and hospitals. *PIPEDA* is based on the federal government's jurisdiction over "the regulation of trade and commerce."

While municipalities, educational institutions and hospitals may occasionally provide services on a fee basis, they are not, on the whole, engaged in trade and commerce as contemplated by the Canadian Constitution. Furthermore, these institutions are completely or largely dependent on municipally or provincially levied taxes and provincial grants.

As a result, our Office is of the view that, as a general rule, *PIPEDA* does not apply to the core activities of municipalities, universities, schools, and hospitals. By core activities we mean those activities that are central to the mandate and responsibilities of these institutions.

Providing a service for a fee does not necessarily trigger the application of the *Act* if the service is part of the institution's core activities. For example, charging a fee for a private room or charging extra for a fiberglass cast does not automatically make a hospital or even that transaction subject to the *Act*. Similarly, a municipality can charge a per bag fee to collect garbage without becoming subject to the *Act*.

A municipality, university, school or hospital may become subject to the *Act* when it engages in a non-core commercial activity. For example, if a university sold or bartered an alumni list, that activity would be considered a commercial activity and that particular transaction would be subject to the *Act*. As well, personal information collected by a university or a hospital in the course of operating a parking garage would probably be subject to the *Act* since this would not be considered a core activity.

A coffee shop in a hospital or university, a TV rental service in a hospital, a university bookstore or any other business operated by third party within one of these institutions would be subject to the *Act* just as a coffee shop in a shopping mall is subject to the *Act*, unless it is in a province with substantially similar legislation.

Private educational institutions and private hospitals are in a different situation. These institutions are more clearly engaged in commercial activities and we would recommend that they operate on the assumption that they are subject to *PIPEDA*.

The Health Care Sector

The core activities of public hospitals or publicly funded long-term care facilities are not subject to *PIPEDA*. However, health care providers in private practice such as doctors, dentists and chiropractors are engaged in a commercial activity and thus subject to the *Act*. For additional information on the application of *PIPEDA* to the health care sector see http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00207e.html.

Provincial Legislation

In some provinces, personal information collected by municipalities, universities, schools and hospitals is protected by provincial public sector legislation. Alberta, Saskatchewan, Manitoba and Ontario have enacted personal health information legislation that applies to the health care sector, including hospitals.

The Territories

The situation in the three Territories is somewhat more complex. *PIPEDA* applies to all federal works, undertakings and businesses (FWUBs) and to the personal information of employees of FWUBs. A FWUB is "any work, undertaking or business that is within the legislative authority of Parliament.

Since all organizations in the Territories are considered to be FWUBs, *PIPEDA* applies to information about employees of municipalities, universities, schools and hospitals in the Territories.

However, *PIPEDA* does not apply to patient or student information in publicly funded hospitals or schools in the Territories because they are not considered to be engaged in commercial activities.

Last Updated: 2004-12-03 ▲ Important Notices

PIPEDA Awareness Raising Tools (PARTs) Initiative For The Health Sector

Questions & Answers

- What's New
- Provincial / Territorial Legislation
- Health & Privacy
- Investigative Bodies
- International Issues
- Background Material
- Related Links

NOTICE: This document has been prepared in consultation with health care provider associations within the context of their day-to-day activities in providing care and treatment to Canadians. The answers to the questions may not necessarily be appropriate for organizations not subject to PIPEDA.

[PDF version 214KB]

Overview
Key Definitions
Scope of Application
Knowledge and Consent
Disclosure
Use and Retention
Access
Safeguards

This document is an administrative tool to assist in understanding PIPEDA. It is not intended as legal advice.

Overview: ▲

1. **What is the "*Personal Information Protection and Electronic Documents Act*" (PIPEDA)?**

   PIPEDA is federal legislation that protects personal information, including health information. It sets out ten principles that organizations, individuals, associations, partnerships and trade unions must follow when collecting, using and disclosing personal information in the course of a commercial activity.

2. **Does PIPEDA apply throughout Canada?**

   The Act will not apply to personal information in Provinces and Territories that have substantially similar privacy legislation in place covering commercial activities that are provincially/territorially regulated. PIPEDA does not apply within the province of Quebec because the province has received substantially similar status but the Act will continue to apply to the province of Quebec for personal information sent outside of the province and to organizations currently subject to the Act, such as banks, broadcasters, airlines, transportation companies and other federally regulated organizations. For more details on this subject please consult Industry Canada's web site.

3. **(a) What are the core features of PIPEDA?**

The core features of PIPEDA include: obtaining consent and identifying the purpose for the collection of personal information, procuring additional consent, express consent in some cases, for any secondary uses or disclosures of the information. To make the consent valid, the Act requires communicating to individuals what personal information is being collected, and how it will be used, disclosed, and protected (see answer #38).

(b) What are PIPEDA's key principles?

The 10 key principles of PIPEDA are listed below. The Q&As that follow will show how these elements apply in the health sector.

a. Organizations are accountable for the protection of personal health information under their control.
b. The purposes for which the personal information is being collected must be identified during or prior to the collection.
c. Information must be collected with the knowledge and consent of the individual and for a reasonable purpose.
d. The collection of personal information is to be limited to what is necessary for the identified purposes and will be collected by fair and lawful means.
e. Information can only be used and disclosed for the purpose for which it was collected and will be retained only as long as it is necessary to fulfil the purpose.
f. Information must be as accurate, complete and up-to-date as possible.
g. Information must be protected by adequate safeguards.
h. Information about an organization's privacy policies and practices is to be readily available.
i. Information must be accessible for review and correction by the individual whose personal information it is, and;
j. Organizations are to provide the means to an individual to challenge an organization's compliance of the above principles.

* Organizations include associations, partnerships, trade unions, agencies, and institutions. It also includes health care providers in private practice.

4. **Why is this law required?**

PIPEDA aims to provide assurances to the public, patients, and providers that personal health information will continue to be managed and shared confidentially and securely.

The Government of Canada believes that, in most cases, PIPEDA's principles may not significantly differ from those currently in place in the health sector. However, to make consent valid PIPEDA requires informing patients of their privacy rights and providing them with an opportunity to know what personal information is being collected, for what purpose, how it will be used, disclosed, and protected (see answer #38).

5. **What additional responsibilities will be added to health professionals as a result of PIPEDA?**

PIPEDA should have minimal impact on regulated health professionals involved in commercial activities who already have good privacy and confidentiality practices in place. Most health professionals already work within a legislative framework or code of ethics that requires them to protect patient privacy, and PIPEDA supports most current best practices.

Health professionals will have to ensure that they:

- Let patients know about the collection, use or disclosure of their personal information. (see question #38)
- Obtain consent to disclose information to third parties when appropriate.
- Provide an individual with access to his or her own personal information.
- Provide secure storage of information and implement measures to limit access to patient records.
- Ensure proper destruction of information that is no longer necessary.
- Inform patients of the organization's information-handling practices through various means (i.e. the posting of notices, brochures and pamphlets, and/or through normal discussions between a patient and a health care provider).

6. **Under PIPEDA are privately insured or privately paid health services considered to be commercial activities?**

   PIPEDA does not differentiate between activities based upon who is paying for them. It is based on the nature of the activity. For example, a hospital charging for a fibreglass cast would not bring a hospital within the scope of the Act because the transaction is part of the hospital's core activities, i.e. providing health care services. (see question 24)

   In the case of a privately owned medical equipment store or TV rental business, if the hospital leases the space to the operator, the latter is responsible for complying with the Act, not the hospital.

7. **How does PIPEDA impact the non-commercial aspect of the health care sector?**

   Non-commercial areas of health care such as publicly funded hospitals are not subject to PIPEDA.

8. **Some health care services are delivered in "open concept" offices. Under PIPEDA can care and treatment continue in the open concept?**

   Special attention and discretion must be exercised in collecting, using and disclosing personal information where services are delivered in an open concept.

Key Definitions: ▲

9. **What is personal information?**

   In the health context, personal information means information about an identifiable patient which includes any factual or subjective information, recorded or not, about that individual, including health related information.

10. **What is an organization?**

    An organization includes associations, partnerships, trade unions, agencies, and institutions. It also includes health care providers in private practice.

11. **What is a commercial activity within the context of the health care sector?**

    A commercial activity involves the making and provision of a product or service that is commercial in nature. Under PIPEDA, commercial activities include, for example, the selling, bartering, or leasing of donor,

membership or other fundraising lists for some consideration. The funding source (public health insurance, private payer, 3rd party payer, etc) is not relevant in determining the existence of a commercial activity.

12. **What is a "circle of care"?**

The expression includes the individuals and activities related to the care and treatment of a patient. Thus, it covers the health care providers who deliver care and services for the primary therapeutic benefit of the patient and it covers related activities such as laboratory work and professional or case consultation with other health care providers.

13. **What does "access" mean under PIPEDA?**

Access is not defined in PIPEDA. However, the intention of the right of "access" is to enable individuals to be informed of the existence of, to view and/or obtain a copy of, the personal information, in a form that is generally understandable, that has been collected about them by an organization. The access right also includes the right of individuals to challenge the accuracy and completeness of the information and to have it amended, as appropriate. (see questions # 68 & 69)

14. **PIPEDA uses a "reasonable person" test. What does the term "reasonable person" mean?**

The concept of "reasonable person" is a test that is intended to ensure that personal information is only collected, used or disclosed for purposes that the average person would consider appropriate, logical and fair in the circumstances.

15. **What are an institution's "Core Activities"?**

An institution's "core activities" are those objectives/activities defined either in a provincial Act which regulates that particular industry or those objectives/activities in the legal entity's Letters Patents, including those activities which logically or legally flow from the latter. For example, the core activities of a hospital includes providing accommodations, providing health care services, etc.

Scope of Application: ▲

16. **Does PIPEDA apply to the entire health sector in Canada?**

No, PIPEDA only applies to the information collected, used and disclosed in the course of commercial activities such as private pharmacies, laboratories and health care providers in private practices. Also, the Act will not apply to personal information in Provinces and Territories that have substantially similar privacy legislation in place covering commercial activities that are provincially regulated, such as in the province of Quebec. For more details on this subject please consult Industry Canada's Privacy For Business web site.

17. **Are there significant differences between PIPEDA and current privacy practices in the health sector?**

No, privacy is a right underpinning health care in Canada. This right is addressed in legislation, codes of ethics, standards and procedures. The Government of Canada believes that, in most cases, PIPEDA's principles may not significantly differ from those currently in place in the health sector. However, to make consent valid PIPEDA requires informing patients of their privacy rights and providing them with an opportunity to know what personal information is being collected, for what purpose, how it will be used, disclosed, and protected (see answer #38).

18. **Why must information about the collection, use, and disclosure of personal information be made available to patients?**

    Information about privacy rights must be made available to patients so that the patients can decide whether or not to consent to the collection, use and disclosure of their personal information.

19. **Will PIPEDA impact on health care professionals/providers and health care facilities/services/agencies?**

    PIPEDA should not significantly alter the therapeutic provider/patient relationship. However, PIPEDA may require some changes. For example, in addition to informing individuals about the purpose of the collection, use and disclosure of their personal information to make their consent valid, health care organizations should review their practices and policies to ensure they meet the PIPEDA principles, in particular with respect to secondary uses of the personal health information, e.g. research, health surveillance and statistical analysis of data purposes.

20. **Does PIPEDA require that every health care provider in private practice develop a privacy policy?**

    Yes. However, the effort and resources to develop a privacy policy will vary substantially according to the size and type of organization. For example, in a sole practitioner's office, this could be a short document, available on request that sets out the application of the 10 privacy principles under PIPEDA (See Question 3b).

21. **Does PIPEDA require that every health care provider in private practice appoint a privacy officer?**

    Under PIPEDA, organizations are required to designate an individual or individuals who are accountable for the organization's compliance with PIPEDA. For a sole practitioner's office, the sole practitioner might be the designated accountable individual or administrative staff could take on this role.

22. **Does PIPEDA apply within a circle of care?**

    Yes, it applies to commercial activities within the circle of care.

23. **A number of health care providers work in settings that are not typically thought of as "health care facilities" - for example, schools, correctional facilities, halfway houses, and group homes. Will PIPEDA mean that different privacy rules can apply for different settings?**

    Yes. A key consideration in determining which organization or individual should comply with PIPEDA is who has control of the personal information and whether they are engaged in commercial activity.

    PIPEDA does not apply to core activities of a municipality, public school, university, public hospital or correctional facility. Public sector legislation and provincial health information acts would apply in some cases and in some jurisdictions. For example, the Federal Privacy Act would apply in the case of a federal correctional institution.

    PIPEDA applies to personal information collected, used, and disclosed during the course of any commercial activity. Records in organizations engaged in commercial activity would be covered by PIPEDA, e.g. private group homes.

    In the case of an organization subject to PIPEDA that employs a health care professional on a contract basis or on salaried basis, the issue of accountability for compliance depends on who has control of the personal information - the organization, the professional or both.

24. **Is the application of PIPEDA based on the nature of the activity (transaction) or is it based on the nature (public, private, commercial, non-profit, etc) of the health organization, institution, or agency?**

    It is based on the nature of the activity.

    A non-profit organization can be engaged in a commercial activity to which the Act would apply. For example, the sale of a fundraising list by a charity can trigger the application of the Act with respect to that particular transaction.

    The Act would not apply to a provincially funded hospital. Hospitals are beyond the constitutional scope of the Act as their core activities are not commercial in nature. Charging for a private room would not bring a hospital within the scope of the Act because the transaction is part of the hospital's core activities, i.e. providing accommodation.

    In the case of a privately owned medical equipment store or TV rental business, if the hospital leases the space to the operator, the latter is responsible for complying with the Act, not the hospital.

25. **What is the responsibility of health care providers employed by federal/provincial/territorial governments under PIPEDA?**

    PIPEDA does not apply to federal/provincial/territorial government employees in the execution of their duties. Most federal government institutions, departments, agencies and their employees are subject to the Federal Privacy Act. Provincial/territorial governments are subject to their respective public sector privacy legislation and should be governed accordingly.

26. **Are health care services delivered by long-term care facilities and home health care agencies considered to be commercial activities, which will make them subject to PIPEDA?**

    NOTE: The following answers are preliminary and very general in nature and may vary in particular circumstances depending on the specific circumstances of the situation.

    a. Long-term care facilities

        i. Private for-profit

        Yes. The health care activities carried out by this type of organization would be considered commercial and therefore subject to PIPEDA.

        ii. Private non-profit

        Organizations of this type vary greatly in their corporate objectives and their organizational structure. In order to determine if a specific private non-profit long-term care facility's health care services are commercial activities, which would make them subject to PIPEDA, it is advisable that the organization consult with their legal counsel.

        iii. Provincial (public institution/facility/agency)

        PIPEDA does not apply to core activities of a municipality, public school, university, and public hospital. Public sector legislation and provincial health information acts would apply in some cases and in some jurisdictions. The Act would not apply to a provincial public long-term care facility.

        iv. Federal (public institution/facility/agency)

PIPEDA does not apply to federal government institutions to which the federal Privacy Act applies. Facilities that are unclear on this matter should consult their legal counsel to determine if they are subject to the federal Privacy Act.

v. Municipal homes for the aged

PIPEDA does not apply to core activities of a municipality, public school, university, and public hospital.

vi. Veterans' homes

PIPEDA does not apply to federal government institutions to which the federal Privacy Act applies.

b. Home care services

i. Private for-profit

Yes. The health care activities carried out by this type of organization would be considered commercial and thus subject to PIPEDA. However, it is advisable for organizations to consult with their legal counsel.

ii. Private non-profit

Organizations of this type vary greatly in their corporate objectives and their organizational structure. In order to determine if a specific private non-profit home care agency's health care services are commercial activities, which would make them subject to PIPEDA, it is advisable that the organization consult with their legal counsel.

iii. Provincial (public institution/facility/agency)

PIPEDA does not apply to core activities of a municipality, public school, university, and public hospital. Public sector legislation and provincial health information acts would apply in some cases and in some jurisdictions. PIPEDA would not apply to a provincial public home care agency. (See Question 14)

iv. Federal (public institution/facility/agency)

PIPEDA does not apply to federal government institutions to which the federal Privacy Act applies. Agencies that are unclear on this matter should consult their legal counsel to determine if they are subject to the federal *Privacy Act*.

27. **How will PIPEDA have an impact on health professional regulations?**

Let's remember that PIPEDA applies only in the context of commercial activities. If the health professional regulatory provisions exceed those of PIPEDA then there is no impact. However, if the regulatory provisions are weaker or do not address certain requirements, than PIPEDA would prevail.

28. **In the event that federal privacy legislation is at odds with provincial/territorial laws, standards and codes of practice governing professional associations, which legislation takes precedence? For example, a patient requests a change in his/her file and the regulatory body requires that records not be altered while PIPEDA allows modifications.**

For a true conflict to exist between PIPEDA and provincial legislation, it must be impossible to comply with both requirements.

In the example noted above, one would not alter the document but instead add a notation to the file indicating the patient's view of the matter. If the information in the file were indeed inaccurate, it would be important to note it in the file but also indicate when and how the error was detected.

29. **What impact will PIPEDA have on health facility accreditation, on quality assurance activities, on chart audits for safety, on reviews against performance measures, on programme/service evaluation?**

Where it has been determined that PIPEDA applies to the particular health facility and a review is undertaken to assess and evaluate the care provided to an individual patient, still receiving care in the facility, then this review can be considered to be part of the circle of care.

In instances where a number of charts are reviewed as part of a broader quality assurance program, service evaluation, safety review, accreditation activity, or assessment of broader provider practices, de-identified patient information should be used or patient express consent should be obtained unless an existing provincial law permits these disclosures.

30. **Under PIPEDA, can regulatory bodies/colleges still continue to conduct their investigative practices? Does PIPEDA require any changes in the manner in which these investigative activities are conducted?**

The relationship between a regulatory body/college and its members is most often of a noncommercial nature, and therefore not captured by PIPEDA. These bodies are also generally empowered by law to obtain personal information as necessary to fulfill their various functions. Professionals subject to the authority of a regulatory body/college would in all likelihood have agreed to the use of their personal information by the body, as part of a condition of membership. PIPEDA recognizes such authority.

Regulatory bodies/colleges may, in the course of their function, need to obtain personal information from other organizations that are subject to PIPEDA, such as financial institutions. Such organizations may only disclose personal information without consent to entities that have been designated as "investigative bodies" under PIPEDA, by regulation. As such, regulatory bodies/colleges may be required to obtain this designation if they wish to obtain personal information from these organizations without an individual's consent.

31. **Are regulatory bodies engaged in a "commercial activity" when they collect, use or disclose personal information in the course of carrying out their statutory responsibilities to regulate their members?**

No.

32. **Do health care professional Regulatory Bodies, operating under provincial legislation, have to obtain an investigative body status under PIPEDA in order to continue to conduct complaint investigations?**

Not necessarily. Professional regulatory bodies should first determine if they have adequate authority under existing provincial legislation. If not, they may need to have this authority recognized under PIPEDA.

33. **How can colleges, regulatory bodies and accreditation bodies apply for investigative body status under PIPEDA?**

They can apply for investigative body status under PIPEDA at Industry

Canada. Requests should be directed to:

Director General
Electronic Commerce Branch
Industry Canada
300 Slater Street
Room D2090
Ottawa, Ontario
K1A 0C8

34. **Are there differences in the application of PIPEDA for different insurance plans, whether public or private?**

Health insurance plans that fall within the scope of public sector privacy legislation, such as the Provincial Government Health Insurance Plans, are not subject to PIPEDA. However, organizations selling private health insurance plans must comply with PIPEDA unless they are subject to provincial/territorial legislation that has been deemed substantially similar to PIPEDA. If the information flows outside provincial/territorial borders, PIPEDA will apply.

Health care providers should make their patients aware that they, the providers, send certain information to private health insurance plans. In many cases, patients are required to sign forms to obtain reimbursement for prescription drugs or dental visits, and these forms typically contain consent provisions.

35. **Do co-payments or user fees impact the application of PIPEDA?**

No. The application of PIPEDA depends on the nature and character of the activity that the organization engages in, not the nature of the organization. For example the private practice of a health care provider is a commercial activity. Noncommercial activity is not subject to the Act. The method of payment does not determine whether or not an activity is of a commercial nature.

36. **How are telehealth services impacted by PIPEDA?**

Telehealth is a way of providing direct health services and, as such the same rules apply.

However, telehealth presents increased risk to the security of the information (such as unauthorized access and network breaches). As such, specific safeguard measures (e.g. encryption, access protocols) should be put in place to address these particular risks.

37. **Does PIPEDA apply to the transfer of personal information:**

a) Between provinces and territories?

The transfer of personal information between provinces and territories is subject to PIPEDA if it occurs in the course of a commercial activity.

b) Across international boundaries?

The transfer of personal information outside of Canada to another country is subject to PIPEDA if it occurs in the course of a commercial activity. A provider's responsibilities under PIPEDA, such as ensuring that health information is protected, apply even when sending personal information across an international border.

Knowledge and Consent: ▲

38. **Under PIPEDA, the patient's knowledge of the collection, use and disclosure of their personal health information is required. How**

can this be achieved?

A person can be considered to understand, i.e. be knowledgeable, if they are made aware of their privacy rights including:

- What information is being collected about them
- Purposes for which the information is being collected
- How that information will be used by the provider/health facility/agency
- To whom the provider/health facility/agency will disclose the information
- How the patient can seek access to and corrections to their health record, and;
- How the patient can exercise their right to complain about the organization's personal information practices.

There are several ways of informing patients of these rights, for example, posting of notices, brochures and pamphlets, and/or discussions in the normal course of exchanges that take place between a patient and a health care provider.

Patients should have the opportunity to discuss this information with a health care provider if they wish to do so.

39. **Are there provisions in PIPEDA for compensating health professionals for complying with the legislation?**

No, PIPEDA contains no provision for this or for any of the industry sectors it covers.

40. **Can consent be implied for the use and disclosure of personal health information under PIPEDA?**

Yes, once patients are made aware of their privacy rights (see answer #38), consent is implied if the patient continues to seek care and treatment. Thus current practice of implied consent for the primary use of personal information in the direct care and treatment of an individual patient, as defined in a circle of care, will continue under PIPEDA. For example, a lab may infer consent because the individual would reasonably expect that the results be sent to the provider who ordered the lab work.

41. **Is consent implied for the disclosure of personal health information to private insurance companies or third party payers for the purposes of reimbursement of health services rendered?**

In certain circumstances, yes. In circumstances where the current practice is to obtain written consent by making the patient sign a reimbursement form, the practice should continue. Where no form is signed, implied consent is acceptable provided patients understand that this is happening and have not behaved in a way that may indicate a refusal of consent (see answer #38).

42. **When does PIPEDA require express consent?**

In commercial activities, the patient's oral or written consent is generally required for all uses and disclosures that are not directly related to the care and treatment of a patient.

However, consent is not always required for research purposes. For example, consent is not required if all of the following conditions are met:

- The information is used or disclosed for statistical, scholarly study or research, or purposes that cannot be achieved without using or disclosing the information.

- It is impractical to obtain consent.
- The organization informs the Office of the Privacy Commissioner before the information is used.

43. **What happens when the patient has concerns about the collection, use and/or disclosure of their information with respect to PIPEDA?**

The patient's concerns should be addressed by answering their questions, or providing them with information about privacy policies and practices, . Specific complaints must be received, investigated and addressed, or, if matters are unresolved, individuals must be informed of their right to complain to the Office of the Privacy Commissioner of Canada.

44. **What happens if the patient refuses to give consent?**

The patient must be advised of the known consequences of not consenting. Should the patient continue to refuse to consent, the providers should be guided by their respective professional standards of practice in handling this issue. In some instances, this could result in the denial of health services.

45. **What happens if the patient withdraws consent?**

The patient must be advised of the known consequences of withdrawing consent. In some instances, it could result in the interruption or the non-provision of health services.

It is advisable that the patient's records not be destroyed for as long as they are necessary to maintain patient safety and meet audit, regulatory or other purposes. The organization should record the withdrawal and is responsible for notifying parties to whom it had disclosed the information. The patient's withdrawal of consent should not result in the destruction of the record.

46. **In cases of emergency care, must consent to the collection, use and disclosure of personal information be obtained?**

No. PIPEDA clearly provides exemptions in certain health care emergencies. Examples of such cases are when a patient is unconscious, too sick or not lucid, or when collection is clearly in the interests of the individual and consent cannot be obtained in a timely way.

47. **How do you obtain knowledge and consent if the individual does not understand either English or French, or is visually impaired and you do not have any written material (in other languages or Braille) to give them?**

Reasonable efforts should be made to communicate with the individual in order to obtain consent. Efforts can include communicating in their language, by sign language, or other means (including an interpreter or family member accompanying the patient).

48. **How will PIPEDA affect research that requires access to personal information? Will researchers require patient consent to access their records?**

Under PIPEDA health information collected in the course of a commercial activity can be used and disclosed for research purposes without consent if all the following conditions are met:

- The information is used or disclosed for statistical, scholarly study or research purposes that cannot be achieved without using the information.
- The information is used in a manner that will ensure its

confidentiality.
- It is impractical to obtain consent.
- The organization informs the Office of the Privacy Commissioner of Canada before the information is used or disclosed.

49. **How does PIPEDA's consent requirement affect the reporting requirements of provincial/territorial legislations?**

Reporting requirements, such as reporting the abuse of persons, infectious diseases and danger to others, will not change. The Act allows disclosure without consent when required by law.

50. **Current practice allows that a prescription can be brought, filled, and handed over to a person acting on behalf of another person. Will PIPEDA change this practice? If so, how?**

PIPEDA supports most current best practices. If an individual walks into a pharmacy with a signed prescription from a doctor for another person, they should be asked how they represent that other person. If the answer is reasonable, implied consent can be assumed, since they possess a document that likely was entrusted to them by the individual.

51. **Does PIPEDA change current practices for substitute decision makers who can exercise the right of the individual with respect to access to information and other rights related to collection, use and disclosure of the individual's health information?**

PIPEDA does not change current practices in place for substitute decision makers.

Disclosure: ▲

52. **Can case consultation still be done?**

Yes, PIPEDA does not preclude case consultation among health care providers.

53. **Can personal information be shared without patient consent between providers in an emergency situation?**

Yes.

54. **Pharmacists often print lists of filled prescriptions for patients for income tax purposes. This might include a list of prescriptions used by all members of the family. Is a separate, written consent required from each family member? What about children under the age of majority?**

Yes, express consent, either in writing or verbally, is required from all individuals of majority age. In the case of a child, consent can be obtained from the minor's legal guardian. Note that this example can be extended to other situations and professions in which a provider is asked to produce a listing of services.

55. **Under PIPEDA, can prescriptions still be phoned or faxed in by the prescriber for delivery to the patient?**

Yes. Prescriptions can still be phoned or faxed in by the prescriber for delivery to the patient, on the condition that appropriate security safeguards are in place to protect the information.

56. **If a health professional receives a request from another health professional, can patient information for circle of care purposes be disclosed to the requesting party without the patient's express consent?**

Yes, under PIPEDA, express consent of the patient is not required if the information is disclosed for the care and treatment of the patient within the circle of care.

57. **A third party health benefits insurer may require that a policyholder be made aware of a claim by another person covered under the policyholder's insurance. What is the health care provider to do under these circumstances?**

The onus to obtain the consent of the patient rests with the insurer. If this consent has not been obtained, the provider cannot be made to disclose information to a third party by a commercial contract.

58. **Can drug manufacturers continue to report adverse drug reactions using identifiable patient information to Health Canada without the patient's knowledge and consent?**

Yes. Manufacturers are required, under the *Food and Drugs Act* and its regulations to report all adverse drug reactions. Since the disclosure is "required by law" it is permissible under PIPEDA.

59. **Under PIPEDA, can a health care provider in private practice continue to send billing information that contains identifiable health information without the express consent of a patient for the purposes of reimbursement to:**

The provincial/territorial government;

Yes. Health care providers should inform their patients that they, the providers, are required to send certain information to provincial/territorial government for reimbursement.

A 3rd party payer?

Yes. Health care providers should inform their patients that they, the providers, will be required to send certain information to private health insurance plans in order to be paid for the services rendered. In many cases, patients are required to sign forms to obtain reimbursement for prescription drugs or dental visits, and these forms typically contain consent provisions. (See questions # 41 & 34)

60. **Under PIPEDA, can a health care facility or service operating under the federal/provincial/territorial government e.g. a Health Authority still send, without the express consent of the patient, health record abstracts that contain identifiable information to:**

A. The provincial/territorial government;

Yes, as PIPEDA does not apply to federal/provincial/territorial governments' activities.

B. The Canadian Institute for Health Information (CIHI)?

Yes, as PIPEDA does not apply to federal/provincial/territorial governments' activities. For more information on CIHI, please see http://secure.cihi.ca/cihiweb/splash.html.

Use and Retention: ▲

61. **How does PIPEDA impact on the retention of temporary recordings of information?**

Under PIPEDA all identifiable personal information, regardless of format, must be protected in the same way. Temporary records that are

no longer required can be destroyed, or modified to ensure that the information is no longer identifiable.

If the provider uses a third party organization to transcribe personal information, the provider is obligated to use contractual agreements to ensure that the information is adequately protected by the third party organization in accordance with PIPEDA.

62. **Patients sessions are sometimes videotaped or audio taped for educational and clinical purposes. Training tapes are typically destroyed and do not form part of the patient's record. What impact will PIPEDA have on this practice?**

PIPEDA supports most current best practices. Patient consent must be obtained before taping. The consent form should indicate the retention period for the tape.

Educational tapes that identify individuals must be considered to be their personal information. However, some note must be made of the existence of the tape to enable the individual to have access to the tape. If an individual asks to have access to the tape they would have to be given access to the portion containing footage of themselves only.

63. **How does PIPEDA impact on the ability of health care facilities to send fundraising letters to patients?**

Fundraising, in this context, is not considered to be a commercial activity. Therefore there would be no impact from PIPEDA on this activity, unless the facility was selling, leasing or trading the fundraising lists for some consideration. (see question #11).

64. **Health professionals often have the financial value of their practice assessed through a review of patient health records. Under PIPEDA can this practice continue?**

Yes. This would be considered a transfer for processing purposes, for which consent is not required. The health professional must ensure that the personal information is protected while in the possession of the third party conducting the valuation.

65. **Under PIPEDA, can a provincial/territorial government use, without the express consent of the patient, the identifiable health information, which has been collected as a result of reimbursement for care and treatment or from other sources, such as, health record abstracts for administration/management, activities such as, planning, resource allocation, reporting, policy development or evaluation?**

PIPEDA does not apply to federal/provincial/territorial governments' activities. The personal health information collected by the governments, regardless of the source or reason for the collection, should be used and disclosed according to privacy legislation applicable to the public sector.

66. **Under PIPEDA, can a 3rd party payer utilize, for other general administrative purposes, the identifiable health information, which has been collected as a result of reimbursement for care and treatment, without the express consent of the patient?**

No. The use of identifiable health information is limited to the original purpose of the collection for which consent was given. If the information is to be utilized for new purposes, the patient's express consent must be obtained for each new purpose.

67. **A private health care provider/facility has collected identifiable information in the course of care and treatment. It has informed the**

patient that the information may be used for administrative/management activities such as planning resource allocation, reporting, or evaluation. Can the private provider use the information for these stated purposes?

The provider/facility/service should make reasonable efforts to anonymize the patient's identifiable information for purposes of administration/management activities (see question #38).

When the patient has been informed that their identifiable information will be used for specifically identified administration/management activities by the private provider/facility/service agency and the patient continues with the consultation for care and treatment, the patient's consent can be inferred for this use of his/her identifiable information.

Access: ▲

68. **What is required if the patient requests that his/her records be corrected?**

PIPEDA should not alter current best practices. The health care provider will consider the request and decide whether to make the change or not.

Historical data should be maintained as long as necessary to maintain patient safety and meet audit, regulatory or other purposes. The patient's request and the health professional's decision should be noted in the file.

69. **Do patients have a right to demand to have their record changed?**

No, they have a right to seek correction, which will be considered by the health care provider who will decide whether to make the change or not. The lack of change by the provider may then be the subject of a complaint to the Office of the Privacy Commissioner.

70. **Under PIPEDA, can a health professional deny an individual access to his/her own record?**

Yes, access can be denied for several different reasons, including:

- If doing so would likely reveal information about another individual, unless the other individual's information is severable or the other individual third party has consented.
- If doing so could reasonably be expected to threaten the life or security of another individual, unless the third party information is severable.
- If the information is protected by solicitor-client privilege.
- If doing so would reveal confidential commercial information.

71. **Under PIPEDA, can a health professional deny an individual access to his/her own record if the health professional thinks it might harm the individual?**

No, PIPEDA does not allow denial of access for this purpose. If access is denied on this basis, the requester can complain to the Office of the Privacy Commissioner who will investigate.

72. **Under PIPEDA, will patients have access to the interpretation tools used in psychological testing?**

PIPEDA applies to personal information. If the interpretation tools are not or do not contain personal information about the patient, PIPEDA does not apply. However, if the interpretation tools are necessary for the

personal information to be understandable then they must also be released.

For example, if the tool translates raw numbers into a meaningful result, the meaningful result has to be provided, not simply the raw data.

Safeguards: ▲

73. **What is required to comply with the security standards set out in PIPEDA?**

Organizations should assess their current security practices.

As necessary, security provisions include:

- Developing and implementing a security policy to protect personal health information. The effort and resources to accomplish this exercise will vary substantially according the size and type of organization. For a sole practitioner's office, this could simply be a short documentation of how the information is safeguarded such as:
  - physical measures (locked filing cabinets, restricting access to offices, alarm systems)
  - technological tools (passwords, encryption, firewalls, anonymizing software)
  - organizational controls (security clearances, limiting access on a "need-to-know" basis, staff training, confidentiality agreements)
- Making employees aware of the importance of maintaining the security and confidentiality of personal information by holding regular staff training on safeguards.
- Reviewing and updating security measures regularly.

74. **Are home care records subject to PIPEDA?**

Home care records are subject to PIPEDA if there is a commercial activity. However, where the records are in the patient's home and under the patient's control, these records are not the responsibility of the provider organization(s).

75. **Vials and other medication containers with patient and drug name are thrown directly in the trash by some pharmacies. Will there now be an obligation under PIPEDA to erase or destroy in a secure manner this information prior to disposing of the vials/medication containers?**

Yes. Vials and other medication containers that show a patient and drug name are considered personal information, which should be erased or destroyed in a secure manner.

Created: 2004-03-03
Updated: 2004-04-07
▲ top of page
Important Notices
Privacy Statement

Fact Sheets

Protecting Your Privacy on the Internet

Canada's new privacy law

Surfing the Net can be fun and educational.

Email is a great way to stay in touch with family and friends. Chat groups and discussion groups allow you to communicate with people with similar interests.

Most people are aware of the Internet's benefits, but not everyone is aware of how the Internet can threaten personal privacy and the steps you can take to protect your privacy in

The *Personal Information Protection and Electronic Documents Act* came into effect January 1, 2001. It gives you certain rights with respect to the collection, use or disclosure of your personal information by federally regulated organisations. These include airlines, banks, telephone companies, cable television and broadcasting companies, as well as all businesses in Nunavut, the Yukon and the Northwest Territories.

The *Act* applies to personal information collected, used or disclosed in the course of commercial activities, whether in the "real" world or on the Internet. It also applies to personal information disclosed to another province or country for profit or gain, where the information is the subject of the transaction. In 2002, the *Act* will be extended to protect your health information. And in 2004, in addition to covering *all* interprovincial or international disclosures of personal information in the course of a commercial activity, the *Act* will extend to *all* provincially regulated businesses not covered by a provincial law judged to be substantially similar to the *Act*.

The *Act* specifies what information a Web site can collect from you, and how. It also specifies how this information can be used. As well, it gives you control over how your personal information, including your email address, is used.

The *Act* also gives you the right to gain access to and correct information a Web site has about you.

Under the *Act*, you have the right to make a complaint to the Privacy Commissioner of Canada if:

- you run into any difficulties obtaining your personal information;
- an organization covered by the *Act* refuses to correct information you consider inaccurate or incomplete;
- you suspect your personal information has been improperly collected, used or disclosed; or
- if you believe an organization is not following any provision of the law.

Visit the following links for discussions about how to protect your privacy when surfing the Net.

On the Web

Chat, Discussion and News Groups

Electronic mail

Resources

Glossary

On the Web

What can happen:

Many Web sites collect personal information-some are just more obvious about it.

Some Web sites ask for personal information before granting entry, such as your full name, age, address, telephone number, and even questions about your personal preferences.

Other Web sites collect information in more subtle ways. Some search engines remember what you have looked for by keeping track of the words you type in the search box.

Many Web sites put one or more "cookies" on your hard drive. Cookies are small text files that can collect and store information such as:

- the Internet Protocol (IP) address of your computer;
- the operating system you are using;
- banner ads you've clicked on;
- Web sites you've visited; and
- any information such as your name that you may voluntarily provide.

This information allows Web sites to identify you the next time you visit. This makes it unnecessary for you to identify yourself every time you visit a Web site and it allows it to provide customized information such as the sports scores of your favourite teams.

However, cookies also enable Web sites or advertising networks to create a profile of you based on the information you have provided and your browsing patterns, often for advertising purposes.

Your information may be forwarded to an advertiser who selects advertisements to pop up on your screen designed to appeal specifically to you. Advertisers may also use this information to send email ads for products or services they think you might like.

Organizations covered by the *Personal Information Protection and Electronic Documents Act* are required to protect your personal information with appropriate safeguards, whether the information is in a database accessible through the Internet, or in a filing cabinet.

However, media stories about hackers gaining access to supposedly secure Web sites containing credit card numbers and other personal information suggest that few, if any Web sites, are completely secure.

In a perfect world, companies would protect your personal information. Unfortunately, this is not the case. Below are some tips on how you can do this yourself.

What you can do:

- Refuse some or all of the cookies that Web sites send you. Check your browser's "help" files to find out how to program your computer to do this. Remember some Web sites can make it difficult or even impossible for you to visit them if you don't accept their cookies.

  For more detailed instructions on how to detect and reject cookies, visit our privacy policy.

- Be cautious about the information you provide to Web sites. They may use this information for marketing purposes.

- Reduce the amount of personal information that you provide to Web sites. Don't provide any information that is not required. Some financial institutions are now offering options like one-time credit card numbers for Web purchases to offer greater security.
- Before you buy anything or make a financial transaction online, read the Web site's privacy policy. If it doesn't have one, think twice about making the transaction. Check opt-out boxes that limit the use of any information you provide.

Chat, Discussion and News Groups

What can happen:

If you take part in chat groups, anyone from the simply curious to potential employers can search for copies of your messages, which can be kept indefinitely. It is possible to find the names of chat or discussion groups in which you participate, and the names of news groups to which you subscribe. The names of those groups alone can reveal a lot about you.

What you can do:

- Participate in chat or discussion groups under a fake name. Check the Resources listed below.
- Be discreet. As a general rule, assume that your online communications are not private unless they are encrypted.
- Some groups that store your old messages allow you to delete them for good: do it!

Electronic mail

What can happen:

The amount of unsolicited, junk email you receive as a result of your travels around the Web can be an annoyance, but this "spam" is only the most obvious privacy problem.

Any email message you send or receive can be intercepted along the way and read–even changed–by anyone from your Internet service provider to the police.

Even deleted email messages can be read from your computer hard disk or someone else's.

It's also possible for other people to send messages under your name, expressing opinions or ordering items without your knowledge, and leaving you to deal with whatever problems that might cause.

What you can do:

- Think of email as post cards–unsealed messages that others can read or pass on to someone else. If you want to communicate privately, install software that allows you to "encrypt" or scramble your email messages so nobody can understand them except you and the person you're writing to (see Resources).
- Send your messages through anonymous remailers, organizations that remove your identity from messages before sending them on to their destination.
- Use email software that lets you control who can see the messages you send–and for how long.
- Ask your Internet service provider to have junk email deleted before it gets to your mailbox. It's likely a few will still sneak through; if this happens, delete the messages without opening them. If you have opened them, don't answer them.
- Many junk email messages offer the opportunity to "remove you" from their list: **Don't do it!** By responding, you confirm your email address is good, and whoever sent you the junk email can sell that address to even more advertisers.

Resources

The following Web sites provide additional information about online privacy issues, including information about privacy tools such as encryption, anonymous remailers and software for anonymous browsing:

www.epic.org

www.privacyexchange.org

www.privacyrights.org

Glossary

Anonymous browsing–several companies offer software, some of it free, that allows you to create online fake names so you can browse Web sites, exchange emails and participate in chat groups anonymously.

Anonymous remailers–organizations that forward your email to its destination after removing any information that could trace it back to you.

Banner ads–Web site advertisements, often in the form of a bar or banner across the top of the screen or a button that you click on for more information. When you see a banner ad appear, a cookie is usually being added to your hard drive.

Chat groups–two or more users communicating in real time with computers via the Internet. The group can consist of two people or dozens. Chat groups take place in either public or private chat rooms. The conversations can be a free-for-all or a structured discussion on a prearranged topic.

Cookies–small text files that are placed on your computer's hard drive when you visit Web sites. Cookies collect and store information about you based on your browsing patterns and information you provide.

There are two kinds of cookies that a Web site can use. **Persistent cookies** are stored on your hard drive for many months or years. **Per-session cookies** are cached (stored in memory) during your visit to the Web site and are automatically deleted from your computer when you disconnect from the Internet.

Privacy seals–seals of approval granted by organizations such as TRUSTe, BBBOnline and WebTrust. The seals are intended to demonstrate that a Web site has adopted appropriate policies to protect personal information and to assure individuals that they are visiting a Web site they can trust. Disclaimer–keep in mind that these seals are not monitored and *anyone* can "stick" a seal on their Web site.

For more information, contact:

The Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, ON
K1A 1H3
info@privcom.gc.ca
www.privcom.gc.ca
1-800-282-1376

July 2001

Last Updated: 2004-03-31 Important Notices

Fact Sheets

Best Practices for the use of Social Insurance Numbers in the private sector

Should businesses ask individuals for their Social Insurance Number?

The Office of the Privacy Commissioner of Canada has long held the position that the Social Insurance Number (SIN) should not be used as a general identifier and that organizations should restrict their collection, use and disclosure of SINs to legislated purposes.

While recognizing that some private-sector organizations are required by law to request customers' or employees' SINs, we remain opposed in principle to the practice of requesting the SIN for general purposes of identification. We recommend that no private sector organization request the SIN from a customer, and that no customer give the SIN to a private-sector organization, unless the organization is required by law to request it.

To what extent is collection of SINs permissible in the private sector?

- Employers are authorized to collect SINs from employees in order to provide them with records of employment and T-4 slips for income tax and Canada Pension Plan (CPP) purposes.
- Organizations such as banks, credit unions, brokers and trust companies are required under the *Income Tax Act* to ask for customers' SINs for tax reporting purposes (e.g., interest earning accounts, RRSPs, etc.).
- No private-sector organization is legally authorized to request customers' SINs for purposes other than income reporting. Even in the case of a financial institution, if a customer's account is not of a type that earns interest (e.g., if it is a credit account as opposed to a savings account), there is no legal requirement for the organization to collect the individual's SIN, and no obligation for the individual to supply it.
- Even so, there is no law prohibiting an organization from asking for a customer's SIN, or a customer from supplying the SIN, for purposes other than income reporting.

Although we do not recommend the practice, we recognize that an organization may ask for the SIN, and a customer may choose to supply it, for reasonable purposes of identification, provided that the principles of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) are duly observed.

How does *PIPEDA* apply to the collection, use, and disclosure of SINs?

A SIN is the personal information of the individual to which it is assigned. As such, its collection, use, or disclosure is subject to all relevant provisions of *PIPEDA*. Notably, the following principles of Schedule 1 to *PIPEDA* apply.

- *Principle 4.2 (Identifying purposes):* An organization must inform the individual of its purposes for collecting the SIN and should do so at the time of collection, either orally or in writing (e.g., on an application form).
    - The organization should clearly specify whether it is requesting the SIN for purposes of income-reporting or for purposes of identification.
    - If requesting the SIN for purposes of income reporting, the organization should clearly indicate that the request is required by law.
    - If requesting the SIN only for purposes of identification, the organization should clearly indicate that the collection is optional.
    - If an organization that is required to collect the SIN for income-reporting purposes intends to use it also for purposes of identification, the organization should, at the time of collection, clearly specify this further intention and clearly indicate that the individual's consent to the identification purposes is optional.
    - An organization must not use the SIN for any purpose not previously identified without first specifying the new purpose and obtaining the individual's express consent to it. In other words, if the organization originally specified only income-reporting as the purpose for collecting the SIN, it must again seek the individual's consent before using the SIN for purposes of identification.
    - Where the SIN is to be used for purposes of identification, an organization must provide a convenient mechanism whereby the individual may withdraw consent to such purposes any time after providing the SIN. The mechanism should be inexpensive, easy to execute, and immediately effective. A toll-free telephone number is recommended.
- *Principle 4.3 (Consent):* The knowledge and consent of the individual are required for any collection, use, or disclosure of a SIN. Where purposes for collecting the SIN are reasonable and clearly specified to the individual at the time of collection (e.g., on an application form), the organization may take the individual's provision of the SIN as indication of consent.
- *Principle 4.3.3* : "An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes."
    - Identification purposes are not in themselves considered a legitimate basis for requiring an individual to provide the SIN. If the SIN is being requested for purposes of identification only, the organization must not in any way suggest to the individual that the SIN is required as a condition for providing a product or service or otherwise establishing a business relationship.
    - Even where it is reasonable for an organization to ask a customer for proof of identity, a request for the SIN in particular must be represented and treated as optional. In verifying identity, an organization may request the SIN as one option among others, but never as a requirement in itself.
    - When banks or other credit-granting institutions need to confirm identity for the purposes of running a credit check on a loan applicant, it is acceptable to ask for the SIN as one among several identification options, but it should not be required as a condition for granting credit.

Fact Sheets

Social Insurance Numbers (SIN)

What is the Social Insurance Number (SIN)?

The Social Insurance Number (SIN) was created in 1964 to serve as a client account number in the administration of the Canada Pension Plan and Canada's varied employment insurance programs. In 1967, what is now Canada Customs and Revenue Agency (CCRA) started using the SIN for tax reporting purposes.

Why do organizations ask for it?

Organizations in and outside government ask for the SIN because it is a simple method of identification. Many use it as a client account number to save them from setting up their own numbering systems.

Although only certain government departments and programs are authorized to collect and use the SIN, there is no legislation that prohibits organizations asking for it.

Why is my SIN so important to personal information and privacy?

- The SIN may be a key piece of information to open the door to your personal information.
- Computer technology makes it possible to use the SIN to find and match your information from one database to another; without your knowledge, a detailed profile could be drawn about you. This amounts to "data surveillance" or monitoring of your daily life, which can pose a serious threat to our privacy and autonomy.
- Your SIN can be used to steal your identity. Along with other personal information, someone may be able to use your SIN to apply for a credit card or open a bank account, rent vehicles, equipment, or accommodation in your name, leaving you responsible for the bills, charges, bad checks, and taxes.

Who can ask for my SIN?

Your SIN is a confidential number that is restricted to income-related information. There are a *select and limited number* of federal government departments and programs specifically authorized to collect the SIN. See list below.

The authority to collect and use the SIN is tied to a specific legislated purpose, *not* necessarily to a particular body. For example, an employer can collect an employee's SIN to provide them with Records of Employment and T-4 slips for income tax purposes, as can provincial or municipal agencies to report financial assistance payments for income tax purposes.

Institutions from which you earn interest or income, such as banks, credit unions and trust companies, must also ask for your SIN.

So, what can I do when asked for my SIN?

- Ask if you are required by law to provide it (see list below);
- Ask why the person needs it, how it will be used and to whom it will be given;
- Your SIN is not a piece of identification. If it is not required by law (and you are not satisfied with the explanation), tell the person you prefer not to use the SIN and offer other identification;

- If the organization refuses to give you the product or service unless you give your SIN, complain to the Privacy Commissioner of Canada;
- If you would like better legal protection for your SIN, call or write your federal Member of Parliament.

Do any provincial and municipal safeguards exist?

While most provincial and municipal governments may not be prohibited from collecting and using the SIN, many are reviewing their use of it and considering alternatives. All provinces and territories have privacy laws to protect personal information in government files.

If you are concerned about how your provincial government is using the SIN, contact your provincial information and privacy commissioner and find out more.

How am I protected in the private sector?

The *Personal Information Protection and Electronic Documents (PIPED) Act* sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities.

The *Act* currently applies to personal information about customers or employees that is collected, used or disclosed by the federally-regulated sector in the course of commercial activities. It also applies to information that is sold across provincial and territorial boundaries. As of January 1, 2004, the *Act* will cover the collection, use and disclosure of personal information in the course of any commercial activity within a province, including provincially-regulated organizations, except in provinces that have enacted legislation that is deemed to be substantially similar to the federal law.

Under the new law, organizations like banks, telecommunications companies and airlines cannot require you to consent to the collection, use or disclosure of your personal information unless it is required for a specific and legitimate purpose.

This means that unless an organization can demonstrate that your SIN is required by law, or that no alternative identifier would suffice to complete the transaction, you cannot be denied a product or service on the grounds of your refusal to provide your SIN.

If you disagree with a request for your SIN made by an organization that is subject to the *PIPED Act*, you can complain to the Privacy Commissioner of Canada, who will investigate the complaint.

At present, only Quebec has provincial legislation that regulates private sector use of personal information.

Legislated uses of the SIN (or legislation that regulates its use) include:

- Canada Pension Plan, Old Age Security and Employment Insurance contributions or claims (the original purposes for the SIN);
- Income Tax identification;
- banks, trust companies, caisse populaires and stock brokers when they sell you financial products (GICs or Canada Savings Bonds) or services (bank accounts) that generate interest. They declare your interest to Canada Customs and Revenue Agency (CCRA) for income tax purposes;
- various Veterans Affairs benefit programs;
- Canada Student Loans or Canada Student Financial Assistance;
- Canada Education Savings Grants;
- Gasoline and Aviation Gasoline Excise Tax Applications;
- Canadian Wheat Board Act;
- Labour Adjustment Benefits Act;
- Tax Rebate Discounting Regulations;
- Race Track Supervision Regulations;
- Garnishment Regulations (Family Orders and Agreements Enforcement Assistance Act);
- Canada Elections Act;

- Canadian Labour Standards Regulations (Canada Labour Code);
- Farm Income Protection.

Programs Authorized to use the SIN:

- Immigration Adjustment Assistance Program;
- Income and Health Care Programs;
- Income Tax Appeals and Adverse Decisions;
- Labour Adjustment Review Board;
- National Dose Registry for Occupational Exposures to Radiation;
- Rural and Native Housing Program;
- Social Assistance and Economic Development Program

For more information about privacy and your SIN, call toll free 1-800-282-1376, or write:

The Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, ON
K1A 1H3

Visit the Human Resources and Development Web site to find answers to general questions about the SIN - such as how to apply for a SIN, or replace a lost or stolen card.

Last Updated: 2004-03-31 ▲ Important Notices

Fact Sheets

Identity Theft: What it is and what you can do about it

Every year, thousands of people are victims of identity theft.

While recent developments in telecommunications and computer processing make it easier for companies and consumers to reach each other, they can also scatter your personal information more widely, making life easier for criminals.

Identity theft is the unauthorized collection and use of your personal information, usually for criminal purposes.

Your name, date of birth, address, credit card, Social Insurance Number (SIN) and other personal identification numbers can be used to open credit card and bank accounts, redirect mail, establish cellular phone service, rent vehicles, equipment, or accommodation, and even secure employment.

If this happens, you could be left with the bills, charges, bad cheques, and taxes.

How to fight identity theft

- Minimize the risk. Be careful about sharing personal information or letting it circulate freely.
- When you are asked to provide personal information, ask how it will be used, why it is needed, who will be sharing it and how it will be safeguarded.
- Give out no more than the minimum, and carry the least possible with you.
- Be particularly careful about your SIN; it is an important key to your identity, especially in credit reports and computer databases.
- Don't give your credit card number on the telephone, by electronic mail, or to a voice mailbox, unless you know the person with whom you're communicating or you initiated the communication yourself, and you know that the communication channel is secure.
- Take advantage of technologies that enhance your security and privacy when you use the Internet, such as digital signatures, data encryption, and "anonymizing" services.
- Pay attention to your billing cycle. If credit card or utility bills fail to arrive, contact the companies to ensure that they have not been illicitly redirected.
- Notify creditors immediately if your identification or credit cards are lost or stolen.
- Access your credit report from a credit reporting agency once a year to ensure it's accurate and doesn't include debts or activities you haven't authorized or incurred.
- Ask that your accounts require passwords before any inquiries or changes can be made, whenever possible.
- Choose difficult passwords -- *not* your mother's maiden name. Memorise them, change them often. *Don't* write them down and leave them in your wallet, or some equally obvious place.
- Key in personal identification numbers privately when you use direct purchase terminals, bank machines, or telephones.
- Find out if your cardholder agreement offers protection from credit card fraud; you may be able to avoid taking on the identity thief's debts.
- Be careful what you throw out. Burn or shred personal financial information such as statements, credit card offers, receipts, insurance forms, etc. Insist that businesses you deal with do the same.

Are you a victim of identity theft?

- Report the crime to the police *immediately*. Ask for a copy of the police report so that you can provide proof of the theft to the organizations that you will have to contact later.
- Take steps to undo the damage. Avoid "credit-repair" companies: there is usually nothing they can do, and some have been known to propose a solution—establishing credit under a new identity—that is itself fraudulent.
- Document the steps you take and the expenses you incur to clear your name and re-establish your credit.
- Cancel your credit cards and get new ones issued. Ask the creditors about accounts tampered with or opened fraudulently in your name.
- Have your credit report annotated to reflect the identity theft. Do a follow-up check three months after to ensure that someone has not tried to use your identity again.
- Close your bank accounts and open new ones. Insist on password-only access to them.
- Get new bank machine and telephone calling cards, with new passwords or personal identification numbers.
- In the case of passport theft, advise the Passport Office.
- Contact Canada Post if you suspect that someone is diverting your mail.
- Advise your telephone, cable, and utilities that someone using your name could try to open new accounts fraudulently.
- Get a new driver's licence.

If you suspect that someone has been using your SIN to get a job, or that your SIN has been compromised in some other way, contact Human Resources Development Canada at:

Social Insurance Registration
P.O. Box 7000
Bathurst, NB E2A 4T1
E-mail: sin-nas@hrdc-drhc.gc.ca

To find out more about your privacy rights, call the Office of the Privacy Commissioner of Canada toll-free at 1-800-282-1376, or write:

The Office of the Privacy Commissioner
112 Kent Street
Ottawa, ON K1A 1H3
E-mail: info@privcom.gc.ca

Last Updated: 2004-03-31 ▲ Important Notices

Fact Sheets

Application of the *Personal Information Protection and Electronic Documents Act* to Employee Records

You may be wondering how the *Personal Information Protection and Electronic Documents Act* applies to employment in the private sector.

The *Act* applies to personal information about employees of an organization that collects, uses, or discloses the information in connection with the operation of a federal work, undertaking, or business — that is, any work, undertaking, or business that falls within the legislative authority of the Parliament of Canada, such as the following:

- Telecommunications
- Broadcasting
- Interprovincial or international trucking, shipping, railways, or other transportation
- Aviation
- Banking
- Nuclear energy
- Activities related to maritime navigation and shipping (including, for example, ports and longshoring)
- Local businesses in Yukon, Nunavut, and the Territories (where all private sector activity is in federal jurisdiction).

The *Act* applies to employment in these industries, as well as to employment in Federal Crown corporations bound by order under the Act.

You may also be wondering about changes after January 1, 2004. As of that date, wherever substantially similar provincial legislation doesn't apply, the *Act* applies to all organizations in Canada that collect, use, or disclose personal information in the course of commercial activities.

So will the *Act* apply to employment in all organizations in Canada? No, it will not.

The *Act* aplies to employee information *only* in organizations that are engaged in federal works, undertakings or businesses. The extension of the Act's scope in 2004 does not change that.

For organizations engaged in federal works, undertakings or businesses, what does the *Act* mean for employer-employee relationships?

The *Act* recognizes two fundamental points: individuals have a right to privacy with respect to their personal information, and organizations need to collect, use, and disclose personal information for appropriate purposes. Compliance with the *Act* requires that these two realities mesh.

Employers in federal works, undertakings or businesses must ensure that they collect, use, and disclose employees' personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

Employers need to respect the ten principles set out in Schedule 1 of the Act, as modified or clarified in the *Act* itself:

1. **Accountability:** the employer is responsible for the personal information under its control, and must designate someone who is accountable for its compliance with the

Act.

2. **Identifying purposes:** the employer must specify why it is collecting personal information from employees at or before the time it does so.
3. **Consent:** the employee's knowledge and consent is required for the collection, use, or disclosure of personal information. (The *Act* permits certain specific exceptions to this principle).
4. **Limiting collection:** employers may only collect the personal information that's necessary for the purpose they've identified, and must collect it by fair and lawful means.
5. **Limiting use, disclosure, and retention:** unless they have the consent of the employee, or are legally required to do otherwise, employers may use or disclose personal information only for the purposes for which they collected it, and they may retain it only as long as necessary for those purposes. (Again, the *Act* permits exceptions.)
6. **Accuracy:** the employees' personal information must be accurate, complete, and up-to-date.
7. **Safeguards:** personal information must be protected by appropriate security safeguards.
8. **Openness:** the employer must make its personal information policies and practices known to its employees.
9. **Individual access:** employees must be able to access personal information about themselves, and be able to challenge the accuracy and completeness of it. (The *Act* permits some exceptions.)
10. **Challenging compliance:** employees must be able to present a challenge about the employer's compliance with the *Act* to the person that the employer has designated as accountable.

Complaints under the *Act*

Employees in federal works, undertakings, or businesses who think that their employer has not respected the provisions of the *Act* should try to resolve the matter internally. If this does not work, they may file a complaint with the Privacy Commissioner, who acts as a "privacy ombudsman". The Commissioner will investigate and try to resolve the matter, as appropriate. If they are dissatisfied with the outcome of the Commissioner's investigation, in some cases they can apply to the Federal Court for a hearing of the complaint.

A final note

Employers whose employee information is not covered by the *Personal Information Protection and Electronic Documents Act* can still benefit from informing themselves about it.

Organizations covered by the *Act* for their customer information may wish to consider extending the same protections to their employee information. The principles of the *Act* are widely accepted both in Canada and internationally as the basis of ethical personal information practices. Employers with international operations who have to comply with privacy legislation in other countries will find the *Act* a helpful guide. In Canada, several provinces have passed privacy laws that apply to employment, and more are expected to do so. Many of these laws are or will be substantially similar to the *Personal Information Protection and Electronic Documents Act*. Understanding the federal *Act* can also give organizations a head start on compliance with future provincial legislation.

Last Updated: 2004-03-31 ▲ Important Notices

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada
Canada

Fact Sheets

Privacy in the Workplace

Employers and employees are often subject to privacy laws. The *Privacy Act*, for example, applies to employee information in federal government institutions. The *Personal Information Protection and Electronic Documents Act* applies to employee information in federal works, undertakings, and businesses. See our fact sheet entitled Application of the PIPEDA to Employee Records. Several provinces have privacy legislation applying to employee information. In addition, employers often make a commitment in collective agreements to observe privacy practices.

But whether or not privacy is protected by law or contract, respecting privacy in the workplace makes good business sense.

People expect to have some privacy at work, even if they are on their employer's premises and using the employer's equipment. At the same time, it's normal that working for someone will mean giving up some privacy. Employers need basic information about their employees for things like pay and benefits, and they have to be able to ensure that work is being done efficiently and safely.

But the possibilities for infringing on privacy are greater than ever before. Psychological tests, web-browsing records, video surveillance, keystroke monitoring, genetic testing: the information an employer can have about employees is limitless.

Employers can balance their "need to know" with their employees' right to privacy, if they ensure that they collect, use, and disclose personal information about their employees for appropriate purposes only.

Respecting employees' privacy

An employer's need for information should be balanced with an employee's right to privacy. For almost all personal information — including pay and benefit records, formal and informal personnel files, video or audio tapes, and records of web-browsing, electronic mail, and keystrokes — the following basic rules help to establish and maintain that balance:

- The employer should say what personal information it collects from employees, why it collects it, and what it does with it.
- Collection, use, or disclosure of personal information should normally be done only with an employee's knowledge and consent.
- The employer should only collect personal information that's necessary for its stated purpose, and collect it by fair and lawful means.
- The employer should normally use or disclose personal information only for the purposes that it collected it for, and keep it only as long as it's needed for those purposes, unless it has the employee's consent to do something else with it, or is legally required to use or disclose it for other purposes.
- Employees' personal information needs to be accurate, complete, and up-to-date.
- Employees should be able to access their personal information, and be able to challenge the accuracy and completeness of it.

Do employees' privacy rights conflict with an employer's right to manage?

Employers have legitimate requirements for personal information about their employees. They need to know who they're hiring. They need to address performance issues and ensure the physical security of their workplace. And they may see electronic monitoring and other surveillance as necessary to ensure productivity, stop leaks of confidential information, and

prevent workplace harassment.

So sometimes employers have to delve into private matters. But they can keep those instances to a minimum, and limit the impact on personal privacy. The possibility that an individual employee might do something harmful doesn't justify treating all employees as suspects. The questionable benefit of knowing what every employee is doing on company time and equipment, at all times, needs to be weighed against the cost — including the cost to staff morale and trust. Preventing workplace harassment is an important goal, but it's best achieved through workforce training and sensitization, explicit anti-harassment policies, and appropriate remedial measures when harassment is reported or reasonably suspected, rather than by depriving everyone of their privacy rights.

Clear policies and clear expectations

At a minimum, employers should tell their employees what personal information will be collected, used, and disclosed. They should inform employees of their policies on Web, e-mail, and telephone use, for example. If employees are subject to random or continuous surveillance, they need to be told so.

Employers should also ensure that information they collect for one purpose isn't used for an unrelated purpose without the employee's consent.

Even if they're not required to do so by law, employers should give employees access to the personal information held about them, so that they can verify, and if necessary challenge, its accuracy and completeness.

What about employees who waive their privacy rights?

Employers may be tempted to advise employees or prospective employees that they have no expectations of privacy in the workplace — that the loss of privacy is a condition of employment. Someone who agrees to work under these conditions, it could be argued, has consented to unlimited collection, use, and disclosure of their personal information.

Whether this is really consent — clear, informed, voluntary consent — is questionable. And the general principle of collecting only the personal information that's required for appropriate purposes gets lost with this approach. A better alternative is to specifically ask employees to consent to explicit, limited, and justified collections, uses, and disclosures of their personal information.

A "privacy culture"

In many workplaces, practices like the ones outlined above are required by law, and employees have legal means to assert their rights. Employees may also have enforceable rights to privacy under collective agreements.

But good privacy practice is not just about avoiding complaints, grievances, or lawsuits. Whether or not privacy is protected by law or contract, fostering a workplace culture where privacy is valued and respected contributes to morale and mutual trust, and makes good business sense.

Last Updated: 2004-03-31 ▲ Important Notices

Fact Sheets

Faxing Personal Information

Faxing personal information may increase the risk that highly sensitive details will fall into the hands of people who should not receive them.

What are the risks?

Dialing a wrong fax number could accidentally send sensitive personal information, welfare files, unemployment claims, criminal records or medical diagnoses, to the wrong person. On several occasions employees have misdialled numbers or hit the wrong speed-dial key and sent sensitive personal information to the media.

Locating a fax machine out in the open means personal information being sent or received may be visible to passers-by.

Fax transmissions, like telephone calls, can be tapped and monitored. If you must fax personal information, consider buying a machine which encrypts transmissions.

How can I reduce the risk?

- Fax only personal information that must be transmitted immediately. Send other urgent information by hand.
- Always confirm that the receiver has taken appropriate precautions to prevent anyone else from seeing the faxed documents.
- Before sending a fax, check that the receiver's number is correct, then verify in the machine's display window that you have keyed it in correctly.
- If you must send personal information, always complete the fax cover sheet, clearly identifying both sender and intended receiver. The cover sheet should include a warning that the information is intended for the named recipient only, as well as a request to contact you if the transmission was misdirected.
- Call the recipient to verify that he or she received the complete transmission.
- Any fax machine used to send or receive personal information should be kept in a closed area to prevent unauthorized persons from seeing the documents.
- Consider making one individual responsible for the fax machine. Otherwise, limit the chances that passers-by can see personal documents by sending the documents yourself. Arrange a time to receive faxes containing personal information so you can be at the machine as they arrive.
- Fax only the personal information which you would feel comfortable discussing over the telephone.
- If your fax machine is equipped, use the feature requiring the receiver to enter a password before the machine will print the fax. This ensures that only the intended receiver can retrieve the document. Similarly, ask the sender to make sure that you must supply a password to retrieve the document.
- If you are sending personal information by a fax modem (a fax device contained in a computer), confirm that other users of the computer system cannot get access to the fax without a password. Likewise, if you are expecting information by fax modem, ensure that other users of your system cannot access the information without a password.

What should I do if someone asks me to fax his or her own personal information?

- Explain how faxing personal information can result in it being accidentally disclosed or

deliberately intercepted by other people.

- Explain the risks and the precautions you have taken to reduce the risks. Ensure the person consented before you fax personal information.

Last Updated: 2004-03-31 ▲ Important Notices

Fact Sheets

Best Practices for Recording of Customer Telephone Calls

Justification for Tape Recording

Taping telephone calls involves the collection of personal information. Therefore, the practice should meet fair information practices. In the case of organizations subject to the *Personal Information Protection and Electronic Documents (PIPED) Act*, this form of collection must comply with the legislation:

- Organizations should only record calls for specified purposes;
- Those purposes must meet the reasonable person test;
- Organizations must make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used;
- The individual must consent;
- The information collected should only be used for the specified purposes; and
- The tapes should be subject to the other provisions of the *Act* with respect to matters such as safeguards, access, retention and disposal.

The bottom line is that conversations should not be taped unless it is "for purposes that a reasonable person would consider are appropriate in the circumstances." The individual must be informed of the taping and the purposes for it and the individual has to consent, except in those limited cases where consent is not required. Otherwise, the tape recording of customer telephone calls is unauthorized collection of personal information.

Taping Procedures

In order to comply with the *PIPED Act*, organizations should take the following steps when recording conversations:

1. The individual should be informed that the conversation is being recorded at the beginning of the call. This can be done by an automated recording or by the customer service representative.
2. The individual should be informed of the purpose. The organization must be clear about the purposes; an organization should not state that it is recording the conversation for quality assurance purposes if, in fact, the recording might be used for other purposes. This could be done in a variety of ways - verbally, by pressing a number on the keypad (in the case of automated messages) or with clear messages on monthly statements. (For example: If you have any questions about your bill please call 1-800-XXX-XXXX. Please note your call will be recorded for...) If the individual proceeds knowing the conversation is being recorded and the purpose of the recording, consent is implied.
3. The organization should offer alternatives if the caller objects. The alternatives might involve not taping the call; visiting a retail outlet; writing a letter; or, conducting the transaction over the Internet.

Other Privacy Implications

The recording of customer calls by organizations raises several other privacy issues. Although a customer service representative could attempt to write down the details of a conversation, a recording is qualitatively different for a number of reasons:

- It will capture incidental information that the service representative might not note - information that may not be germane to the call but could be used by the organization

for other purposes;

- It will capture the caller's tone of voice, that could also be used for other purposes such as a legal proceeding; and
- It can be used to infer information about the caller, for example ethnic origin and age that is not relevant to the purpose of the call.

Last Updated: 2004-03-31 ▲ Important Notices

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada
Canada

Fact Sheets

A Day in the Life

...or how to help build your superfile.

Nothing to hide? It's just as well...from the time we get up in the morning until we climb into bed at night we leave a trail of data behind us for others to collect, merge, analyze, massage and even sell, often without our knowledge or consent.

8:30 Exit apartment parking lot?cameras, and possibly a card, record departure.

8:35 Pull onto toll highway?device records your entry and exit points to send bill at the end of the month.

8:42 Caught in traffic jam, call work to delay meeting?cellular phone calls can be easily intercepted; new personal telephones signal your whereabouts to satellites to deliver calls.

9:17 Enter office parking lot?card records entry and time, cameras monitor garage.

9:20 Enter main office/plant door?"Swipe" cards record comings and goings; active badges allow others to locate you anywhere in the building.

9:25 Log on to computer?system records time in.

9:29 Send personal e-mail to friend, business message to colleague?both can be read by the employer; simple deletion does not erase them from the computer's hard drive.

10:45 Call your mother?supervisors may monitor phone calls.

11:00 Make a delivery using company vehicle?many company vehicles have geo-positioning devices to plot vehicle location; some have *"black boxes"* to record driving habits.

12:05 Stop at bank machine?system records details of transactions, cameras overhead or in machine record your behaviour.

12:10 Buy birthday gift for friend?credit card records details of purchase, retailer's loyalty card profiles purchase for points and directed discounts; banks may use spending patterns to help assemble complete customer profile.

12:35 Doctor's appointment?health cards will soon contain small computer chips to record your complete medical history on the card, blood samples contain DNA which could be tested for wide variety of conditions, doctor's diagnosis may need to be disclosed to insurance company if you buy life or disability insurance and details sent to centralized registry run by insurance companies.

1:15 Pick up prescription?some provinces have on-line drug networks which share your drug history with pharmacies across the province and may be disclosed to police tracking drug abuse.

1:30 Return to work?card records your return.

2:45 Provide urine sample for employer's new drug testing program?reveals use of targeted drugs but not impairment; sample may also reveal use of legal drugs such as birth control pills, insulin and anti-depressants.

3:30 Meeting in secure area?pass through security which scans retina to confirm identity.

5:30 Complete first draft of report?computer records content, can also store keyboard speed, error rate, length of pauses and absences.

6:15 Leave office?exit recorded by computer, entry system and parking lot.

6:30 Buy groceries?debit card purchase recorded, loyalty card tracks selections for marketing and targeted discounts.

6:45 Pick up video?computer records viewing preferences, Social Insurance Number; store may sell your viewing preferences, say erotica, to other companies.

7:20 Listen to phone messages?your phone has recorded callers' phone numbers, displays your number when you call others, unless you enter code to block the display.

8:20 Order clothing from catalogue?company records personal details and credit card number and may sell the information to database-list-marketers.

8:30 Subscribe to new magazine?many magazines routinely sell their subscribers' list to mass mailers.

8:35 Survey company calls?company gathers political views, social attitudes and personal views. Some surveys are actually marketing calls to collect personal data for future sales. Legitimate surveys destroy personal identifiers once data processed.

8:45 Political canvasser at the door?political contributions of more than $100, amounts and the party, are listed in public records.

9:10 Log onto Internet?your choice of chat groups and your messages can be monitored and a profile assembled by anyone, including police; some Web sites monitor your visits.

Increasingly, living a modern urban life seems to mean there is nowhere to hide. In our search for security and convenience, are we hitching ourselves to an electronic leash?

Originally published in ***The Privacy Commissioner of Canada's Annual Report 1995-96***.

Last Updated: 2004-03-31 ▲ Important Notices

Fact Sheets

What Canadians Can Do to Protect Their Personal Information Transferred Across Borders

Canadians benefit from a reasonable standard of protection of their personal information. They do not want to see that protection vanish when personal information about them is transferred across borders, and they do not want to see governments or organizations in Canada transfer their information across borders if it will be put at risk of inappropriate disclosure, whether for security or for commercial purposes.

The extent to which personal information about Canadians should be made available to foreign governments is a complex issue of continuing concern. Nonetheless, Canadians can take some measures to protect their personal information from inappropriate disclosure to foreign governments:

- By bringing complaints about the handling of personal information (especially outsourcing arrangements) to the Office of the Privacy Commissioner of Canada or provincial and territorial commissioners, depending on the organization whose conduct has raised the concern;
- By relying on the "whistle blowing" provisions of *PIPEDA* if a US based affiliate of a Canadian organization seeks to reach into Canada to obtain personal information held in a Canadian database in order to comply with a US legal order. These provisions would protect the confidentiality of employees who notify the Privacy Commissioner of Canada that a company intends to transfer information abroad in violation of *PIPEDA*. The provisions also protect employees against retaliation by the employers, such as harassment, dismissal or demotion;
- By letting organizations in Canada that collect personal information about Canadians know that there is a concern about personal information being processed outside Canada;
- By taking advantage of the information rights existing under *PIPEDA* and provincial private sector statutes which require organizations to follow fair information practices, notably obtaining consent for information use;
- By reminding companies in Canada of their legal obligation to introduce appropriate security measures to prevent their subsidiaries or affiliates in another country from secretly obtaining access to personal information held in Canada to comply with a court order made in the foreign country;
- By raising their concerns about the potential for excessive disclosure of personal information to foreign governments or to foreign companies with their elected representatives; and
- Generally, by being more attentive to what may be happening to their personal information when it crosses borders and to the importance of clear and enforceable international standards on information sharing in democratic countries.

What Companies Do to Protect the Personal Information of

Canadians Transferred Across Borders

Companies that are subject to *PIPEDA* or similar provincial legislation must comply with that legislation. It is important for the management of organizations subject to such laws to understand their responsibilities under the laws — for example, the obligations in *PIPEDA* to ensure the security of personal information. *PIPEDA* requires personal information to be protected by security safeguards appropriate to the sensitivity of the information.

Corporate leaders increasingly recognize that maintaining a high level of public trust in how personal information is handled is vital to achieve customer loyalty. It is also abundantly clear to corporate leaders that personal information holdings are key business assets that need to be protected against misuse.

Last Updated: 2004-08-18 ▲ Important Notices

Fact Sheets

Best Practices for dealing with pre-PIPEDA personal information (grandfathering)

How does the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) apply to personal information collected before the Act came into effect?

The answer, in brief, is that all provisions of *PIPEDA*, including the consent principle, apply to all personal information held by an organization, regardless of when the information was collected. This means, among other things, that organizations are required to keep the information as accurate, complete and up-to-date as necessary, protect the information with appropriate safeguards and give individuals access to their personal information.

However, it does not necessarily follow that an organization must seek established customers' *express* consent to the continued retention, use or disclosure of their personal information.

Although the guidelines that follow are primarily intended to deal with customer information collected prior to the implementation of *PIPEDA*, they are equally appropriate for information relating to clients, employees, donors and other individuals, keeping in mind that *PIPEDA* only applies to employee information collected, used or disclosed by federal works, undertakings or businesses.

Purging obsolete files

In some cases, destroying or erasing older files may be the most appropriate and straightforward way to deal with them.

Under Principle 4.5 of the Act, an organization should retain personal information only as long as necessary for the fulfillment of the purposes for which it was collected; should develop guidelines and procedures regarding retention, including minimum and maximum retention periods; and should destroy or erase any personal information no longer required to fulfil identified purposes.

In determining how to treat an existing customer file, an organization should first consider such questions as:

- Is the information still serving (or has it ever served) any purpose that could reasonably be considered necessary or useful;
- Is there a legal or contractual requirement to retain the information: and
- Would the individual reasonably expect the organization to be still holding the information on file?

If the answer to any of these questions is no then the most appropriate action may be simply to purge the file. The organization should also set reasonable minimum and maximum retention periods for handling all customer files in

future.

Seeking Consent

The extent to which an organization is obliged to seek express consent from established customers depends on several considerations:

- Whether the organization made a reasonable effort to inform the customer of its purposes at the time of collecting the personal information;
- Whether the information is still being used or disclosed, and if so whether it is being used or disclosed for the same purposes for which it was collected;
- Whether the information is being used or disclosed for unidentified secondary purposes; and
- Whether the customer would reasonably expect the organization to continue using or disclosing the information for its current purposes.

These considerations relate to the purposes for which the information is being used or disclosed, the degree to which these purposes were specified at the time of collection and the reasonable expectations of the individual.

Purposes duly specified

If the organization made a reasonable effort to specify its purposes to customers at the time of collecting personal information, and if the information is still being used or disclosed for those original purposes and no others, then the organization may take the customers' consent to the purposes as implied. Provided that the information is not used or disclosed for new purposes, there is no further requirement to obtain consent.

Purposes unspecified but reasonably expected

Even if purposes were not clearly specified at the time, but if they were such as customers would reasonably have expected to be involved in the provision of the products or services concerned, then the organization may take customers' consent to the purposes as implied. (The use of personal information to fulfill a magazine subscription is an obvious example.) No further consent is required unless the organization intends to use or disclose the information for new purposes.

Purposes unspecified and not reasonably expected

If the personal information was collected for unspecified purposes that customers would not have reasonably expected to be involved in the provision of the products or services concerned (e.g., secondary purposes such as marketing or disclosures to third parties), then the organization must obtain the customers' express consent to any continued use or disclosure of the information.

New purposes

Regardless of whether the personal information was collected before or after *PIPEDA* took effect, an organization must seek customers' consent to any new use or disclosure of their personal information. A new use or disclosure is defined as any use or disclosure for purposes other than those for which personal information was originally collected.

Access to personal information

Under Principle 4.9 of *PIPEDA* , an organization must, upon request, inform individuals of the existence, use, and disclosure of their personal information, give them access to such information, and enable them to challenge its accuracy and completeness and, if required, have it amended.

This principle applies to all personal information held by an organization, regardless of when it was collected. Customers have a clear right of access to personal information collected by an organization before it became subject to *PIPEDA* .

Making privacy policies available

Under Principles 4.1 and 4.8 of *PIPEDA* , an organization must formulate privacy policies and practices and make information about them readily available to individuals.

These principles apply as much to an organization's established customers as to its new customers. It is recommended that organizations provide privacy information to new customers on the first occasion of collecting personal information from them, and to established customers at the earliest opportunity in the usual course of business communications.

Last Updated: 2004-08-19 ▲ Important Notices

The Digital Economy in Canada

- What's New
- Provincial / Territorial Legislation
- Health & Privacy
- Investigative Bodies
- International Issues
- Background Material
- Related Links

PIPEDA Awareness Raising Tools (PARTs) Initiative For The Health Sector

On January 1, 2004, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) came into full force and effect, covering all collections, uses and disclosures of personal information in the course of commercial activity. The Government of Canada has developed tools to assist organizations in the healthcare sector understand the scope and requirements of the PIPEDA. These tools were prepared in consultation with the Office of the Privacy Commissioner of Canada, as well as major healthcare associations.

The following documents provide basic information on the PIPEDA and on its application to the healthcare sector.

Questions and Answers

Glossary of Terms

Posters and Brochures

For more information see the following sections:

- Substantially Similar Information
- Investigative Bodies
- International Issues
- Background Material
- Related Links

- Go Back to Trust & Confidence Home

▸ What's New
▸ Provincial / Territorial Legislation
▸ Health & Privacy
▸ Investigative Bodies
▸ International Issues
▸ Background Material
▸ Related Links

PIPEDA Awareness Raising Tools (PARTs) Initiative For The Health Sector

Questions & Answers

NOTICE: This document has been prepared in consultation with health care provider associations within the context of their day-to-day activities in providing care and treatment to Canadians. The answers to the questions may not necessarily be appropriate for organizations not subject to PIPEDA.

[PDF version 214KB]

Overview
Key Definitions
Scope of Application
Knowledge and Consent
Disclosure
Use and Retention
Access
Safeguards

This document is an administrative tool to assist in understanding PIPEDA. It is not intended as legal advice.

Overview: ▲

1. **What is the "*Personal Information Protection and Electronic Documents Act*" (PIPEDA)?**

   PIPEDA is federal legislation that protects personal information, including health information. It sets out ten principles that organizations, individuals, associations, partnerships and trade unions must follow when collecting, using and disclosing personal information in the course of a commercial activity.

2. **Does PIPEDA apply throughout Canada?**

   The Act will not apply to personal information in Provinces and Territories that have substantially similar privacy legislation in place covering commercial activities that are provincially/territorially regulated. PIPEDA does not apply within the province of Quebec because the province has received substantially similar status but the Act will continue to apply to the province of Quebec for personal information sent outside of the province and to organizations currently subject to the Act, such as banks, broadcasters, airlines, transportation companies and other federally regulated organizations. For more details on this subject please consult Industry Canada's web site.

3. **(a) What are the core features of PIPEDA?**

   The core features of PIPEDA include: obtaining consent and identifying the purpose for the collection of personal information, procuring additional consent, express consent in some cases, for any secondary uses or disclosures of the information. To make the consent valid, the Act requires communicating to individuals what personal information is being collected, and how it will be used, disclosed, and protected (see answer #38).

   (b) What are PIPEDA's key principles?

   The 10 key principles of PIPEDA are listed below. The Q&As that follow will show how

these elements apply in the health sector.

a. Organizations are accountable for the protection of personal health information under their control.
b. The purposes for which the personal information is being collected must be identified during or prior to the collection.
c. Information must be collected with the knowledge and consent of the individual and for a reasonable purpose.
d. The collection of personal information is to be limited to what is necessary for the identified purposes and will be collected by fair and lawful means.
e. Information can only be used and disclosed for the purpose for which it was collected and will be retained only as long as it is necessary to fulfil the purpose.
f. Information must be as accurate, complete and up-to-date as possible.
g. Information must be protected by adequate safeguards.
h. Information about an organization's privacy policies and practices is to be readily available.
i. Information must be accessible for review and correction by the individual whose personal information it is, and;
j. Organizations are to provide the means to an individual to challenge an organization's compliance of the above principles.

* Organizations include associations, partnerships, trade unions, agencies, and institutions. It also includes health care providers in private practice.

4. **Why is this law required?**

PIPEDA aims to provide assurances to the public, patients, and providers that personal health information will continue to be managed and shared confidentially and securely.

The Government of Canada believes that, in most cases, PIPEDA's principles may not significantly differ from those currently in place in the health sector. However, to make consent valid PIPEDA requires informing patients of their privacy rights and providing them with an opportunity to know what personal information is being collected, for what purpose, how it will be used, disclosed, and protected (see answer #38).

5. **What additional responsibilities will be added to health professionals as a result of PIPEDA?**

PIPEDA should have minimal impact on regulated health professionals involved in commercial activities who already have good privacy and confidentiality practices in place. Most health professionals already work within a legislative framework or code of ethics that requires them to protect patient privacy, and PIPEDA supports most current best practices.

Health professionals will have to ensure that they:

- Let patients know about the collection, use or disclosure of their personal information. (see question #38)
- Obtain consent to disclose information to third parties when appropriate.
- Provide an individual with access to his or her own personal information.
- Provide secure storage of information and implement measures to limit to patient records.
- Ensure proper destruction of information that is no longer necessary.
- Inform patients of the organization's information-handling practices through various means (i.e. the posting of notices, brochures and pamphlets, and/or through normal discussions between a patient and a health care provider).

6. **Under PIPEDA are privately insured or privately paid health services considered to be commercial activities?**

PIPEDA does not differentiate between activities based upon who is paying for them. It is based on the nature of the activity. For example, a hospital charging for a fibreglass cast would not bring a hospital within the scope of the Act because the transaction is part of the hospital's core activities, i.e. providing health care services. (see question 24)

In the case of a privately owned medical equipment store or TV rental business, if the hospital leases the space to the operator, the latter is responsible for complying with the Act, not the hospital.

7. **How does PIPEDA impact the non-commercial aspect of the health care sector?**

Non-commercial areas of health care such as publicly funded hospitals are not subject to PIPEDA.

8. **Some health care services are delivered in "open concept" offices. Under PIPEDA can care and treatment continue in the open concept?**

   Special attention and discretion must be exercised in collecting, using and disclosing personal information where services are delivered in an open concept.

Key Definitions: ▲

9. **What is personal information?**

   In the health context, personal information means information about an identifiable patient which includes any factual or subjective information, recorded or not, about that individual, including health related information.

10. **What is an organization?**

    An organization includes associations, partnerships, trade unions, agencies, and institutions. It also includes health care providers in private practice.

11. **What is a commercial activity within the context of the health care sector?**

    A commercial activity involves the making and provision of a product or service that is commercial in nature. Under PIPEDA, commercial activities include, for example, the selling, bartering, or leasing of donor, membership or other fundraising lists for some consideration. The funding source (public health insurance, private payer, 3rd party payer, etc) is not relevant in determining the existence of a commercial activity.

12. **What is a "circle of care"?**

    The expression includes the individuals and activities related to the care and treatment of a patient. Thus, it covers the health care providers who deliver care and services for the primary therapeutic benefit of the patient and it covers related activities such as laboratory work and professional or case consultation with other health care providers.

13. **What does "access" mean under PIPEDA?**

    Access is not defined in PIPEDA. However, the intention of the right of "access" is to enable individuals to be informed of the existence of, to view and/or obtain a copy of, the personal information, in a form that is generally understandable, that has been collected about them by an organization. The access right also includes the right of individuals to challenge the accuracy and completeness of the information and to have it amended, as appropriate. (see questions # 68 & 69)

14. **PIPEDA uses a "reasonable person" test. What does the term "reasonable person" mean?**

    The concept of "reasonable person" is a test that is intended to ensure that personal information is only collected, used or disclosed for purposes that the average person would consider appropriate, logical and fair in the circumstances.

15. **What are an institution's "Core Activities"?**

    An institution's "core activities" are those objectives/activities defined either in a provincial Act which regulates that particular industry or those objectives/activities in the legal entity's Letters Patents, including those activities which logically or legally flow from the latter. For example, the core activities of a hospital includes providing accommodations, providing health care services, etc.

Scope of Application: ▲

16. **Does PIPEDA apply to the entire health sector in Canada?**

    No, PIPEDA only applies to the information collected, used and disclosed in the course of commercial activities such as private pharmacies, laboratories and health care providers in private practices. Also, the Act will not apply to personal information in Provinces and Territories that have substantially similar privacy legislation in place covering commercial activities that are provincially regulated, such as in the province of Quebec. For more details on this subject please consult Industry Canada's Privacy For Business web site.

17. **Are there significant differences between PIPEDA and current privacy practices in the health sector?**

No, privacy is a right underpinning health care in Canada. This right is addressed in legislation, codes of ethics, standards and procedures. The Government of Canada believes that, in most cases, PIPEDA's principles may not significantly differ from those currently in place in the health sector. However, to make consent valid PIPEDA requires informing patients of their privacy rights and providing them with an opportunity to know what personal information is being collected, for what purpose, how it will be used, disclosed, and protected (see answer #38).

18. **Why must information about the collection, use, and disclosure of personal information be made available to patients?**

Information about privacy rights must be made available to patients so that the patients can decide whether or not to consent to the collection, use and disclosure of their personal information.

19. **Will PIPEDA impact on health care professionals/providers and health care facilities/services/agencies?**

PIPEDA should not significantly alter the therapeutic provider/patient relationship. However, PIPEDA may require some changes. For example, in addition to informing individuals about the purpose of the collection, use and disclosure of their personal information to make their consent valid, health care organizations should review their practices and policies to ensure they meet the PIPEDA principles, in particular with respect to secondary uses of the personal health information, e.g. research, health surveillance and statistical analysis of data purposes.

20. **Does PIPEDA require that every health care provider in private practice develop a privacy policy?**

Yes. However, the effort and resources to develop a privacy policy will vary substantially according to the size and type of organization. For example, in a sole practitioner's office, this could be a short document, available on request that sets out the application of the 10 privacy principles under PIPEDA (See Question 3b).

21. **Does PIPEDA require that every health care provider in private practice appoint a privacy officer?**

Under PIPEDA, organizations are required to designate an individual or individuals who are accountable for the organization's compliance with PIPEDA. For a sole practitioner's office, the sole practitioner might be the designated accountable individual or administrative staff could take on this role.

22. **Does PIPEDA apply within a circle of care?**

Yes, it applies to commercial activities within the circle of care.

23. **A number of health care providers work in settings that are not typically thought of as "health care facilities" - for example, schools, correctional facilities, halfway houses, and group homes. Will PIPEDA mean that different privacy rules can apply for different settings?**

Yes. A key consideration in determining which organization or individual should comply with PIPEDA is who has control of the personal information and whether they are engaged in commercial activity.

PIPEDA does not apply to core activities of a municipality, public school, university, public hospital or correctional facility. Public sector legislation and provincial health information acts would apply in some cases and in some jurisdictions. For example, the Federal Privacy Act would apply in the case of a federal correctional institution.

PIPEDA applies to personal information collected, used, and disclosed during the course of any commercial activity. Records in organizations engaged in commercial activity would be covered by PIPEDA, e.g. private group homes.

In the case of an organization subject to PIPEDA that employs a health care professional on a contract basis or on salaried basis, the issue of accountability for compliance depends on who has control of the personal information - the organization, the professional or both.

24. **Is the application of PIPEDA based on the nature of the activity (transaction) or is it based on the nature (public, private, commercial, non-profit, etc) of the health organization, institution, or agency?**

It is based on the nature of the activity.

A non-profit organization can be engaged in a commercial activity to which the Act

would apply. For example, the sale of a fundraising list by a charity can trigger the application of the Act with respect to that particular transaction.

The Act would not apply to a provincially funded hospital. Hospitals are beyond the constitutional scope of the Act as their core activities are not commercial in nature. Charging for a private room would not bring a hospital within the scope of the Act because the transaction is part of the hospital's core activities, i.e. providing accommodation.

In the case of a privately owned medical equipment store or TV rental business, if the hospital leases the space to the operator, the latter is responsible for complying with the Act, not the hospital.

25. **What is the responsibility of health care providers employed by federal/provincial/territorial governments under PIPEDA?**

PIPEDA does not apply to federal/provincial/territorial government employees in the execution of their duties. Most federal government institutions, departments, agencies and their employees are subject to the Federal Privacy Act. Provincial/territorial governments are subject to their respective public sector privacy legislation and should be governed accordingly.

26. **Are health care services delivered by long-term care facilities and home health care agencies considered to be commercial activities, which will make them subject to PIPEDA?**

NOTE: The following answers are preliminary and very general in nature and may vary in particular circumstances depending on the specific circumstances of the situation.

a. Long-term care facilities

i. Private for-profit

Yes. The health care activities carried out by this type of organization would be considered commercial and therefore subject to PIPEDA.

ii. Private non-profit

Organizations of this type vary greatly in their corporate objectives and their organizational structure. In order to determine if a specific private non-profit long-term care facility's health care services are commercial activities, which would make them subject to PIPEDA, it is advisable that the organization consult with their legal counsel.

iii. Provincial (public institution/facility/agency)

PIPEDA does not apply to core activities of a municipality, public school, university, and public hospital. Public sector legislation and provincial health information acts would apply in some cases and in some jurisdictions. The Act would not apply to a provincial public long-term care facility.

iv. Federal (public institution/facility/agency)

PIPEDA does not apply to federal government institutions to which the federal Privacy Act applies. Facilities that are unclear on this matter should consult their legal counsel to determine if they are subject to the federal Privacy Act.

v. Municipal homes for the aged

PIPEDA does not apply to core activities of a municipality, public school, university, and public hospital.

vi. Veterans' homes

PIPEDA does not apply to federal government institutions to which the federal Privacy Act applies.

b. Home care services

i. Private for-profit

Yes. The health care activities carried out by this type of organization would be considered commercial and thus subject to PIPEDA. However, it is advisable for organizations to consult with their legal counsel.

ii. Private non-profit

Organizations of this type vary greatly in their corporate objectives and their

organizational structure. In order to determine if a specific private non-profit home care agency's health care services are commercial activities, which would make them subject to PIPEDA, it is advisable that the organization consult with their legal counsel.

iii. Provincial (public institution/facility/agency)

PIPEDA does not apply to core activities of a municipality, public school, university, and public hospital. Public sector legislation and provincial health information acts would apply in some cases and in some jurisdictions. PIPEDA would not apply to a provincial public home care agency. (See Question 14)

iv. Federal (public institution/facility/agency)

PIPEDA does not apply to federal government institutions to which the federal Privacy Act applies. Agencies that are unclear on this matter should consult their legal counsel to determine if they are subject to the federal *Privacy Act*.

27. **How will PIPEDA have an impact on health professional regulations?**

Let's remember that PIPEDA applies only in the context of commercial activities. If the health professional regulatory provisions exceed those of PIPEDA then there is no impact. However, if the regulatory provisions are weaker or do not address certain requirements, than PIPEDA would prevail.

28. **In the event that federal privacy legislation is at odds with provincial/territorial laws, standards and codes of practice governing professional associations, which legislation takes precedence? For example, a patient requests a change in his/her file and the regulatory body requires that records not be altered while PIPEDA allows modifications.**

For a true conflict to exist between PIPEDA and provincial legislation, it must be impossible to comply with both requirements.

In the example noted above, one would not alter the document but instead add a notation to the file indicating the patient's view of the matter. If the information in the file were indeed inaccurate, it would be important to note it in the file but also indicate when and how the error was detected.

29. **What impact will PIPEDA have on health facility accreditation, on quality assurance activities, on chart audits for safety, on reviews against performance measures, on programme/service evaluation?**

Where it has been determined that PIPEDA applies to the particular health facility and a review is undertaken to assess and evaluate the care provided to an individual patient, still receiving care in the facility, then this review can be considered to be part of the circle of care.

In instances where a number of charts are reviewed as part of a broader quality assurance program, service evaluation, safety review, accreditation activity, or assessment of broader provider practices, de-identified patient information should be used or patient express consent should be obtained unless an existing provincial law permits these disclosures.

30. **Under PIPEDA, can regulatory bodies/colleges still continue to conduct their investigative practices? Does PIPEDA require any changes in the manner in which these investigative activities are conducted?**

The relationship between a regulatory body/college and its members is most often of a noncommercial nature, and therefore not captured by PIPEDA. These bodies are also generally empowered by law to obtain personal information as necessary to fulfill their various functions. Professionals subject to the authority of a regulatory body/college would in all likelihood have agreed to the use of their personal information by the body, as part of a condition of membership. PIPEDA recognizes such authority.

Regulatory bodies/colleges may, in the course of their function, need to obtain personal information from other organizations that are subject to PIPEDA, such as financial institutions. Such organizations may only disclose personal information without consent to entities that have been designated as "investigative bodies" under PIPEDA, by regulation. As such, regulatory bodies/colleges may be required to obtain this designation if they wish to obtain personal information from these organizations without an individual's consent.

31. **Are regulatory bodies engaged in a "commercial activity" when they collect, use or disclose personal information in the course of carrying out their statutory responsibilities to regulate their members?**

No.

32. **Do health care professional Regulatory Bodies, operating under provincial legislation, have to obtain an investigative body status under PIPEDA in order to continue to conduct complaint investigations?**

Not necessarily. Professional regulatory bodies should first determine if they have adequate authority under existing provincial legislation. If not, they may need to have this authority recognized under PIPEDA.

33. **How can colleges, regulatory bodies and accreditation bodies apply for investigative body status under PIPEDA?**

They can apply for investigative body status under PIPEDA at Industry Canada. Requests should be directed to:

Director General
Electronic Commerce Branch
Industry Canada
300 Slater Street
Room D2090
Ottawa, Ontario
K1A 0C8

34. **Are there differences in the application of PIPEDA for different insurance plans, whether public or private?**

Health insurance plans that fall within the scope of public sector privacy legislation, such as the Provincial Government Health Insurance Plans, are not subject to PIPEDA. However, organizations selling private health insurance plans must comply with PIPEDA unless they are subject to provincial/territorial legislation that has been deemed substantially similar to PIPEDA. If the information flows outside provincial/territorial borders, PIPEDA will apply.

Health care providers should make their patients aware that they, the providers, send certain information to private health insurance plans. In many cases, patients are required to sign forms to obtain reimbursement for prescription drugs or dental visits, and these forms typically contain consent provisions.

35. **Do co-payments or user fees impact the application of PIPEDA?**

No. The application of PIPEDA depends on the nature and character of the activity that the organization engages in, not the nature of the organization. For example the private practice of a health care provider is a commercial activity. Noncommercial activity is not subject to the Act. The method of payment does not determine whether or not an activity is of a commercial nature.

36. **How are telehealth services impacted by PIPEDA?**

Telehealth is a way of providing direct health services and, as such the same rules apply.

However, telehealth presents increased risk to the security of the information (such as unauthorized access and network breaches). As such, specific safeguard measures (e.g. encryption, access protocols) should be put in place to address these particular risks.

37. **Does PIPEDA apply to the transfer of personal information:**

a) Between provinces and territories?

The transfer of personal information between provinces and territories is subject to PIPEDA if it occurs in the course of a commercial activity.

b) Across international boundaries?

The transfer of personal information outside of Canada to another country is subject to PIPEDA if it occurs in the course of a commercial activity. A provider's responsibilities under PIPEDA, such as ensuring that health information is protected, apply even when sending personal information across an international border.

Knowledge and Consent: ▲

38. **Under PIPEDA, the patient's knowledge of the collection, use and disclosure of**

their personal health information is required. How can this be achieved?

A person can be considered to understand, i.e. be knowledgeable, if they are made aware of their privacy rights including:

- What information is being collected about them
- Purposes for which the information is being collected
- How that information will be used by the provider/health facility/agency
- To whom the provider/health facility/agency will disclose the information
- How the patient can seek access to and corrections to their health record, and;
- How the patient can exercise their right to complain about the organization's personal information practices.

There are several ways of informing patients of these rights, for example, posting of notices, brochures and pamphlets, and/or discussions in the normal course of exchanges that take place between a patient and a health care provider.

Patients should have the opportunity to discuss this information with a health care provider if they wish to do so.

39. **Are there provisions in PIPEDA for compensating health professionals for complying with the legislation?**

No, PIPEDA contains no provision for this or for any of the industry sectors it covers.

40. **Can consent be implied for the use and disclosure of personal health information under PIPEDA?**

Yes, once patients are made aware of their privacy rights (see answer #38), consent is implied if the patient continues to seek care and treatment. Thus current practice of implied consent for the primary use of personal information in the direct care and treatment of an individual patient, as defined in a circle of care, will continue under PIPEDA. For example, a lab may infer consent because the individual would reasonably expect that the results be sent to the provider who ordered the lab work.

41. **Is consent implied for the disclosure of personal health information to private insurance companies or third party payers for the purposes of reimbursement of health services rendered?**

In certain circumstances, yes. In circumstances where the current practice is to obtain written consent by making the patient sign a reimbursement form, the practice should continue. Where no form is signed, implied consent is acceptable provided patients understand that this is happening and have not behaved in a way that may indicate a refusal of consent (see answer #38).

42. **When does PIPEDA require express consent?**

In commercial activities, the patient's oral or written consent is generally required for all uses and disclosures that are not directly related to the care and treatment of a patient.

However, consent is not always required for research purposes. For example, consent is not required if all of the following conditions are met:

- The information is used or disclosed for statistical, scholarly study or research, or purposes that cannot be achieved without using or disclosing the information.
- It is impractical to obtain consent.
- The organization informs the Office of the Privacy Commissioner before the information is used.

43. **What happens when the patient has concerns about the collection, use and/or disclosure of their information with respect to PIPEDA?**

The patient's concerns should be addressed by answering their questions, or providing them with information about privacy policies and practices, . Specific complaints must be received, investigated and addressed, or, if matters are unresolved, individuals must be informed of their right to complain to the Office of the Privacy Commissioner of Canada.

44. **What happens if the patient refuses to give consent?**

The patient must be advised of the known consequences of not consenting. Should the patient continue to refuse to consent, the providers should be guided by their respective professional standards of practice in handling this issue. In some instances, this could result in the denial of health services.

45. **What happens if the patient withdraws consent?**

The patient must be advised of the known consequences of withdrawing consent. In some instances, it could result in the interruption or the non-provision of health services.

It is advisable that the patient's records not be destroyed for as long as they are necessary to maintain patient safety and meet audit, regulatory or other purposes. The organization should record the withdrawal and is responsible for notifying parties to whom it had disclosed the information. The patient's withdrawal of consent should not result in the destruction of the record.

46. **In cases of emergency care, must consent to the collection, use and disclosure of personal information be obtained?**

No. PIPEDA clearly provides exemptions in certain health care emergencies. Examples of such cases are when a patient is unconscious, too sick or not lucid, or when collection is clearly in the interests of the individual and consent cannot be obtained in a timely way.

47. **How do you obtain knowledge and consent if the individual does not understand either English or French, or is visually impaired and you do not have any written material (in other languages or Braille) to give them?**

Reasonable efforts should be made to communicate with the individual in order to obtain consent. Efforts can include communicating in their language, by sign language, or other means (including an interpreter or family member accompanying the patient).

48. **How will PIPEDA affect research that requires access to personal information? Will researchers require patient consent to access their records?**

Under PIPEDA health information collected in the course of a commercial activity can be used and disclosed for research purposes without consent if all the following conditions are met:

- The information is used or disclosed for statistical, scholarly study or research purposes that cannot be achieved without using the information.
- The information is used in a manner that will ensure its confidentiality.
- It is impractical to obtain consent.
- The organization informs the Office of the Privacy Commissioner of Canada before the information is used or disclosed.

49. **How does PIPEDA's consent requirement affect the reporting requirements of provincial/territorial legislations?**

Reporting requirements, such as reporting the abuse of persons, infectious diseases and danger to others, will not change. The Act allows disclosure without consent when required by law.

50. **Current practice allows that a prescription can be brought, filled, and handed over to a person acting on behalf of another person. Will PIPEDA change this practice? If so, how?**

PIPEDA supports most current best practices. If an individual walks into a pharmacy with a signed prescription from a doctor for another person, they should be asked how they represent that other person. If the answer is reasonable, implied consent can be assumed, since they possess a document that likely was entrusted to them by the individual.

51. **Does PIPEDA change current practices for substitute decision makers who can exercise the right of the individual with respect to access to information and other rights related to collection, use and disclosure of the individual's health information?**

PIPEDA does not change current practices in place for substitute decision makers.

Disclosure: ▲

52. **Can case consultation still be done?**

Yes, PIPEDA does not preclude case consultation among health care providers.

53. **Can personal information be shared without patient consent between providers in an emergency situation?**

Yes.

54. **Pharmacists often print lists of filled prescriptions for patients for income tax purposes. This might include a list of prescriptions used by all members of the family. Is a separate, written consent required from each family member? What about children under the age of majority?**

Yes, express consent, either in writing or verbally, is required from all individuals of majority age. In the case of a child, consent can be obtained from the minor's legal guardian. Note that this example can be extended to other situations and professions in which a provider is asked to produce a listing of services.

55. **Under PIPEDA, can prescriptions still be phoned or faxed in by the prescriber for delivery to the patient?**

Yes. Prescriptions can still be phoned or faxed in by the prescriber for delivery to the patient, on the condition that appropriate security safeguards are in place to protect the information.

56. **If a health professional receives a request from another health professional, can patient information for circle of care purposes be disclosed to the requesting party without the patient's express consent?**

Yes, under PIPEDA, express consent of the patient is not required if the information is disclosed for the care and treatment of the patient within the circle of care.

57. **A third party health benefits insurer may require that a policyholder be made aware of a claim by another person covered under the policyholder's insurance. What is the health care provider to do under these circumstances?**

The onus to obtain the consent of the patient rests with the insurer. If this consent has not been obtained, the provider cannot be made to disclose information to a third party by a commercial contract.

58. **Can drug manufacturers continue to report adverse drug reactions using identifiable patient information to Health Canada without the patient's knowledge and consent?**

Yes. Manufacturers are required, under the *Food and Drugs Act* and its regulations to report all adverse drug reactions. Since the disclosure is "required by law" it is permissible under PIPEDA.

59. **Under PIPEDA, can a health care provider in private practice continue to send billing information that contains identifiable health information without the express consent of a patient for the purposes of reimbursement to:**

The provincial/territorial government;

Yes. Health care providers should inform their patients that they, the providers, are required to send certain information to provincial/territorial government for reimbursement.

A 3rd party payer?

Yes. Health care providers should inform their patients that they, the providers, will be required to send certain information to private health insurance plans in order to be paid for the services rendered. In many cases, patients are required to sign forms to obtain reimbursement for prescription drugs or dental visits, and these forms typically contain consent provisions. (See questions # 41 & 34)

60. **Under PIPEDA, can a health care facility or service operating under the federal/provincial/territorial government e.g. a Health Authority still send, without the express consent of the patient, health record abstracts that contain identifiable information to:**

A. The provincial/territorial government;

Yes, as PIPEDA does not apply to federal/provincial/territorial governments' activities.

B. The Canadian Institute for Health Information (CIHI)?

Yes, as PIPEDA does not apply to federal/provincial/territorial governments' activities. For more information on CIHI, please see http://secure.cihi.ca/cihiweb/splash.html.

Use and Retention: ▲

61. **How does PIPEDA impact on the retention of temporary recordings of information?**

Under PIPEDA all identifiable personal information, regardless of format, must be protected in the same way. Temporary records that are no longer required can be destroyed, or modified to ensure that the information is no longer identifiable.

If the provider uses a third party organization to transcribe personal information, the provider is obligated to use contractual agreements to ensure that the information is adequately protected by the third party organization in accordance with PIPEDA.

62. **Patients sessions are sometimes videotaped or audio taped for educational and clinical purposes. Training tapes are typically destroyed and do not form part of the patient's record. What impact will PIPEDA have on this practice?**

PIPEDA supports most current best practices. Patient consent must be obtained before taping. The consent form should indicate the retention period for the tape.

Educational tapes that identify individuals must be considered to be their personal information. However, some note must be made of the existence of the tape to enable the individual to have access to the tape. If an individual asks to have access to the tape they would have to be given access to the portion containing footage of themselves only.

63. **How does PIPEDA impact on the ability of health care facilities to send fundraising letters to patients?**

Fundraising, in this context, is not considered to be a commercial activity. Therefore there would be no impact from PIPEDA on this activity, unless the facility was selling, leasing or trading the fundraising lists for some consideration. (see question #11).

64. **Health professionals often have the financial value of their practice assessed through a review of patient health records. Under PIPEDA can this practice continue?**

Yes. This would be considered a transfer for processing purposes, for which consent is not required. The health professional must ensure that the personal information is protected while in the possession of the third party conducting the valuation.

65. **Under PIPEDA, can a provincial/territorial government use, without the express consent of the patient, the identifiable health information, which has been collected as a result of reimbursement for care and treatment or from other sources, such as, health record abstracts for administration/management, activities such as, planning, resource allocation, reporting, policy development or evaluation?**

PIPEDA does not apply to federal/provincial/territorial governments' activities. The personal health information collected by the governments, regardless of the source or reason for the collection, should be used and disclosed according to privacy legislation applicable to the public sector.

66. **Under PIPEDA, can a 3rd party payer utilize, for other general administrative purposes, the identifiable health information, which has been collected as a result of reimbursement for care and treatment, without the express consent of the patient?**

No. The use of identifiable health information is limited to the original purpose of the collection for which consent was given. If the information is to be utilized for new purposes, the patient's express consent must be obtained for each new purpose.

67. **A private health care provider/facility has collected identifiable information in the course of care and treatment. It has informed the patient that the information may be used for administrative/management activities such as planning resource allocation, reporting, or evaluation. Can the private provider use the information for these stated purposes?**

The provider/facility/service should make reasonable efforts to anonymize the patient's identifiable information for purposes of administration/management activities (see question #38).

When the patient has been informed that their identifiable information will be used for specifically identified administration/management activities by the private provider/facility/service agency and the patient continues with the consultation for care and treatment, the patient's consent can be inferred for this use of his/her identifiable information.

Access: ▲

68. **What is required if the patient requests that his/her records be corrected?**

PIPEDA should not alter current best practices. The health care provider will consider the request and decide whether to make the change or not.

Historical data should be maintained as long as necessary to maintain patient safety and meet audit, regulatory or other purposes. The patient's request and the health professional's decision should be noted in the file.

69. **Do patients have a right to demand to have their record changed?**

No, they have a right to seek correction, which will be considered by the health care provider who will decide whether to make the change or not. The lack of change by the provider may then be the subject of a complaint to the Office of the Privacy Commissioner.

70. **Under PIPEDA, can a health professional deny an individual access to his/her own record?**

Yes, access can be denied for several different reasons, including:

- If doing so would likely reveal information about another individual, unless the other individual's information is severable or the other individual third party has consented.
- If doing so could reasonably be expected to threaten the life or security of another individual, unless the third party information is severable.
- If the information is protected by solicitor-client privilege.
- If doing so would reveal confidential commercial information.

71. **Under PIPEDA, can a health professional deny an individual access to his/her own record if the health professional thinks it might harm the individual?**

No, PIPEDA does not allow denial of access for this purpose. If access is denied on this basis, the requester can complain to the Office of the Privacy Commissioner who will investigate.

72. **Under PIPEDA, will patients have access to the interpretation tools used in psychological testing?**

PIPEDA applies to personal information. If the interpretation tools are not or do not contain personal information about the patient, PIPEDA does not apply. However, if the interpretation tools are necessary for the personal information to be understandable then they must also be released.

For example, if the tool translates raw numbers into a meaningful result, the meaningful result has to be provided, not simply the raw data.

Safeguards: ▲

73. **What is required to comply with the security standards set out in PIPEDA?**

Organizations should assess their current security practices.

As necessary, security provisions include:

- Developing and implementing a security policy to protect personal health information. The effort and resources to accomplish this exercise will vary substantially according the size and type of organization. For a sole practitioner's office, this could simply be a short documentation of how the information is safeguarded such as:
  - physical measures (locked filing cabinets, restricting access to offices, alarm systems)
  - technological tools (passwords, encryption, firewalls, anonymizing software)
  - organizational controls (security clearances, limiting access on a "need-to-know" basis, staff training, confidentiality agreements)
- Making employees aware of the importance of maintaining the security and confidentiality of personal information by holding regular staff training on safeguards.

- Reviewing and updating security measures regularly.

74. **Are home care records subject to PIPEDA?**

Home care records are subject to PIPEDA if there is a commercial activity. However, where the records are in the patient's home and under the patient's control, these records are not the responsibility of the provider organization(s).

75. **Vials and other medication containers with patient and drug name are thrown directly in the trash by some pharmacies. Will there now be an obligation under PIPEDA to erase or destroy in a secure manner this information prior to disposing of the vials/medication containers?**

Yes. Vials and other medication containers that show a patient and drug name are considered personal information, which should be erased or destroyed in a secure manner.

Updated: 2004-04-07

▲
top of page

Important Notices
Privacy Statement

TBC 350-58 (Rev. 1990/11)

Info Source Personal Information Request Form

Privacy Act

Step 1
Determine which federal government institution is most likely to hold personal information about you. Decide whether you wish to submit an informal request for the information or a formal request under the *Privacy Act*. If you wish to make an informal request, contact the appropriate institution. The address can likely be found in ***Info Source*** publications which are available across Canada, generally in major public and academic libraries, federal government offices, such as Employment Immigration Centres, and the constituency offices of federal Members of Parliament.

Step 2
To apply for personal information about you under the *Privacy Act*, complete this form. Describe the information being sought and provide any relevant details necessary to help the institution find it. If your require assistance, refer to ***Info Source (Sources of Federal Government Information)*** for a description of personal information banks held by the institution or contact its Privacy Coordinator.

Step 3
Forward the personal information request form to the Privacy Coordinator of the institution holding the information. The address is listed in the "Introduction" to ***Info Source***.

Step 4
When you receive an answer to your request, review the information to determine whether you wish to make a further request under the Act. You also have the right to complain to the Privacy Commissioner should you beleive that you have been denied any of your rights under the Act.

Federal Government Institution

I wish to examine the information ☐ As it is ☐ All in English ☐ All in French

Provide details regarding the information being sought

Method of access preferred ☐ Receive copies of originals ☐ Examine originals in government offices

Name of applicant

Street, address, apartment | City or town

Province | Postal Code | Telephone number

I request access to personal information about myself under the *Privacy Act* as I am a Canadian citizen, permanent resident or another individual, including an inmate, present in Canada.

Signature | Date

Government of Canada / Gouvernement du Canada

Français au verso

Canada

Info Source

Personal Information Request Form

TBC 350-58 (Rev. 1999/11)

For official use only

Privacy Act

Step 1
Determine which federal government institution is most likely to hold personal information about you. Decide whether you wish to submit an informal request for the information or a formal request under the *Privacy Act*. If you wish to make an informal request, contact the appropriate institution. The address can likely be found in ***Info Source*** publications which are available across Canada generally in major public and academic libraries, federal government offices, such as Employment Immigration Centres, and the constituency offices of federal Members of Parliament.

Step 2
To apply for personal information about you under the *Privacy Act*, complete this form. Describe the information being sought and provide any relevant details necessary to help the institution find it. If your require assistance, refer to ***Info Source (Sources of Federal Government Information)*** for a description of personal information banks held by the institution or contact its Privacy Coordinator.

Step 3
Forward the personal information request form to the Privacy Coordinator of the institution holding the information. The address is listed in the introduction to ***Info Source***.

Step 4
When you receive an answer to your request, review the information to determine whether you wish to make a further request under the Act. You also have the right to complain to the Privacy Commissioner should you believe that you have been denied any of your rights under the Act.

Federal Government Institution

I wish to examine the information ☐ All in English ☐ All in French

Provide details regarding the information being sought

Method of access preferred ☐ Receive copies of originals ☐ Examine originals in government offices

Name of applicant

Street address, apartment City or town

Province Postal Code Telephone number

I request access to personal information about myself under the *Privacy Act* as I am a Canadian citizen, permanent resident or another individual, including an inmate, present in Canada.

Signature Date

Government of Canada / Gouvernement du Canada

Français au verso

Canada

Info Source

Loi sur la protection des renseignements personnels

Formule de demande d'accès à des renseignements personnels

CTC 350-58 (Rev. 1990/11)

Réservé à l'administration

1ère étape

Déterminez quelle est l'institution fédérale la plus susceptible de détenir des renseignements personnels à votre sujet. Décidez ensuite si vous voulez obtenir les renseignements de façon officieuse ou si vous préférez présenter une demande officielle en vertu de la *Loi sur la protection des renseignements personnels*. Dans le cas d'une demande officieuse, il suffit de communiquer avec l'institution compétente dont l'adresse devrait figurer dans ***Info Source***. Les publications « ***Info Source*** » sont disponibles à travers le Canada, et en général dans les principales bibliothèques publiques et celles des universités, dans les bureaux du gouvernement fédéral, tels que les Centres d'emploi et d'immigration du Canada, et dans les bureaux de circonscription des députés fédéraux.

2e étape

Pour présenter une demande officielle en vertu de la *Loi sur la protection des renseignements personnels*, vous devez remplir cette formule. Décrivez l'information demandée et fournissez tous les renseignements pertinents afin d'aider l'institution dans ses recherches. Si vous avez besoin d'aide, consultez ***Info Source (Sources de renseignements fédéraux)*** pour y trouver la description des fichiers de renseignements personnels que détient l'institution, ou communiquez avec le coordonnateur de la protection des renseignements personnels de cette institution.

3e étape

Faites parvenir la demande d'accès à des renseignements personnels au coordonnateur de l'institution détenant les renseignements. L'adresse figure dans l'« Introduction » d' ***Info Source***.

4e étape

Dès que vous recevrez réponse à votre demande, examinez les renseignements afin de déterminer s'il y aurait lieu, à votre avis, de faire une autre demande en vertu de la Loi. Vous avez également le droit de présenter une plainte au Commissaire à la protection de la vie privée si vous estimez avoir été privé des droits que vous confère la Loi.

Institution fédérale

Je désire examiner les renseignements

☐ tels quels ☐ en anglais ☐ en français

Précisions sur l'information demandée

Méthode de consultation préférée

☐ Recevoir des copies de l'original ☐ Examiner l'original dans un bureau du gouvernement

Nom de la personne qui fait la demande

Adresse – Numéro, rue, appartement

Ville ou village

Province

Code postal

Numéro de téléphone

En tant que personne visée par la *Loi sur la protection des renseignements personnels* – les citoyens canadiens, résidents permanents et les autres personnes présentes au Canada, y compris les détenus – je demande d'avoir accès à des renseignements personnels qui me concernent.

Signature

Date

Gouvernement du Canada / Government of Canada

English on reverse

Canada

CTC 350-58 (Rév. 1990/11)

Info Source

Loi sur la protection des renseignements personnels

Formule de demande d'accès à des renseignements personnels

1ère étape

Déterminez quelle est l'institution fédérale la plus susceptible de détenir des renseignements personnels à votre sujet. Décidez ensuite si vous voulez obtenir les renseignements de façon officieuse ou si vous préférez présenter une demande officielle en vertu de la *Loi sur la protection des renseignements personnels*. Dans le cas d'une demande officieuse, il suffit de communiquer avec l'institution compétente dont l'adresse devrait figurer dans ***Info Source***. Les publications « ***Info Source*** » sont disponibles à travers le Canada, et en général dans les principales bibliothèques publiques et celles des universités, dans les bureaux du gouvernement fédéral, tels que les Centres d'emploi et d'immigration du Canada, et dans les bureaux de circonscription des députés fédéraux.

2e étape

Pour présenter une demande officielle en vertu de la *Loi sur la protection des renseignements personnels*, vous devez remplir cette formule. Décrivez l'information demandée et fournissez tous les renseignements pertinents afin d'aider l'institution dans ses recherches. Si vous avez besoin d'aide, consultez ***Info Source (Sources de renseignements fédéraux)*** pour y trouver la description des fichiers de renseignements personnels que détient l'institution, ou communiquez avec le coordonnateur de la protection des renseignements personnels de cette institution.

3e étape

Faites parvenir la demande d'accès à des renseignements personnels au coordonnateur de l'institution détenant les renseignements. L'adresse figure dans l'« Introduction » d'***Info Source***.

4e étape

Dès que vous recevrez réponse à votre demande, examinez les renseignements afin de déterminer s'il y aurait lieu, à votre avis, de faire une autre demande en vertu de la Loi. Vous avez également le droit de présenter une plainte au Commissaire à la protection de la vie privée si vous estimez avoir été privé des droits que vous confère la Loi.

Institution fédérale

Je désire examiner les renseignements

☐ tels quels ☐ en anglais ☐ en français

Précisions sur l'information demandée

Méthode de consultation préférée

☐ Recevoir des copies de l'original ☐ Examiner l'original dans un bureau du gouvernement

Nom de la personne qui fait la demande

Adresse – Numéro, rue, appartement

Ville ou village

Province

Code postal

Numéro de téléphone

En tant que personne visée par la *Loi sur la protection des renseignements personnels* – les citoyens canadiens, résidents permanents et les autres personnes présentes au Canada, y compris les détenus – je demande d'avoir accès à des renseignements personnels qui me concernent.

Signature

Date

Gouvernement du Canada Government of Canada

English on reverse

Canada